INDEX

SECURITY ISSUES-2019

1.INTRODUCTION TO SECURITY

- The term "Security" refers to national security or the absence of threat to the state, **internal or external**.
- The term may also refer to **human security** in which case it would include the absence of physical threat to an individual from organized violence.
- It may also expand to include traditional developmental concepts like **food security, health security** and **employment security**.
- In this context, **Internal security** has been defined as the act of keeping peace within the borders of a sovereign state or other self-governing territories, generally by upholding the national law and defending against **internal security** threats.
- A nation may face threats in a number of ways. A majority of these emanate from internal weaknesses.
- In the present world scenario the failure of internal security is the main factor for degradation and instability.
- The rise of contentious politics based on sectarian, ethnic, linguistic and other divisive criteria, is primarily responsible for the many communal and secessionist movements flourishing in India.
- The inherent challenges were posed by the increasing polarisation of social structure and negative social trends. For e.g., unstable government, intragroup rivalries, factionalism, criminalisation of politics, etc.
- The presence of unfriendly neighbours enables the internal conflicts to get external support. The internal turmoil allures and invites the external elements to weaken the State.
- The vested interests exploit these conditions to pursue their own agenda.
- They give ideological support to exasperate this sense of grievance to such an extent that a small minority are willing to become tools in their hands to subvert the stability and security of the country.
- When a State fails to address the external factors it loses its capacity to control the deluge.
- Therefore, the fine linkage of internal security with the external factors makes the situation difficult to tackle with the conventional law and order approach to meet the challenge of internal security threat.

- India is a country marked by enormous diversity, a multitude of cultures, languages, castes, tribes and religious communities, with wide economic disparities and varied levels of political engagement.
- To keep the nation intact, and to do this without compromising on peace, justice, autonomy and ethics, was a major challenge
- There were claims for ownership of India, to belong and be seen to belong, and therefore be offered a fair share of India's resources.
- India witnessed numerous competing assertions of identity, for inclusion or autonomy, sometimes even for secession.
- There have also been efforts to turn away from India, to disown India and claim autonomy or independence.

- India's geo-political situation, neighborhood factor, historical experience with long and treacherous borders and long maritime boundaries make it **highly vulnerable to external threats.**
- On the other side its communal, caste, linguistic and ethnic fault lines, economic deprivation, political conflicts and turmoil provide opportunity for external forces to endanger the internal security of the country.
- This scenario, has taken a turn for the worse in the last two decades.
- Such problems of internal security become difficult to deal within the frame work of law and order without considering the supreme security interest of the country.

CHALLENGES TO INTERNAL SECURITY

The Government's approach is to deal with Left Wing Extremism in a holistic manner, in the areas of **security, development, ensuring rights** and **entitlements of local communities, improvement in governance** and **public perception management**.

- **'Police'** and **'Public Order'** being State subjects, action on maintenance of law and order lies primarily in the domain of the State Governments.
- The **Central Government** closely monitors the situation and supplements and coordinates their efforts in several ways .

On the security front ,

- Providing Central Armed Police Forces (**CAPFs**) and Commando Battalions for Resolute Action (**CoBRA**).
- Sanction of **India Reserve (IR) battalions**.
- Setting up of **Counter Insurgency and Anti Terrorism (CIAT)** schools.
- Modernisation and upgradation of the State Police and their Intelligence apparatus under the Scheme for Modernization of State Police Forces (**MPF scheme**).
- Re-imbursement of security related expenditure under the **Security Related Expenditure (SRE) Scheme**.

- Providing helicopters for anti-naxal operations, assistance in training of State Police through the Ministry of Defence, the Central Police Organisations and the Bureau of Police Research and Development.
- Facilitating **inter-State coordination**.
- Scheme of **Fortified Police stations**.The MHA has sanctioned 400 police stations in 10 LWE affected States.
- **Assistance to Central Agencies** for LWE management Scheme as a sub scheme of the Umbrella Scheme Modernization of Police Forces. Under the Scheme assistance is provided to Central Agencies like CAPFs, Indian Air Force for anti LWE Operations where the States have constraints.
- **Civic Action Programme (CAP)** :Under the Scheme, funds are released to the CAPFs, deployed in LWE affected areas, for conducting various civic activities in welfare of the local people.

On the Socio-Economic Development front

- The **National Rural Employment Guarantee Act (NREGA)** is an important element in providing livelihood support and protection to the poorest of the poor.
- **Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006** recognizes the rights to hold and live in the forest land under the individual or common occupation for habitation or for self-cultivation for livelihood.
- Progress of the various schemes is regularly monitored by **MHA** though meeting and Video Conferencing with the Central Ministries/Departments concerned and State Governments.
- Empowered Committee under Additional Secretary(LWE),constituted on May 26,2015 has conducted number of meeting with different Ministries in 2017 reviewing the progress/Status of various development Schemes/Projects.

- Compensation to Left Wing Extremist cadres who surrendered in accordance with the **surrender and rehabilitation policy** of the concerned State Government.
- **Special Central Assistance (SCA)** for 35 most LWE affected districts. The main **objective** of the Scheme is to fill the critical gaps in Public Infrastructure and Services, which are of emergent nature.
- **Special Infrastructure Scheme (SIS)** including construction of 250 Fortified Police Stations in LWE affected states. The Scheme **aims** at capacity building of states by strengthening the security apparatus of the States. 250 Fortified Police Stations are also envisaged under the Scheme.

- **Road Requirement Plan-I (RRP-I)** for improving road connectivity in 34 LWE affected districts of 8 States i.e. Andhra Pradesh, Bihar, Chhattisgarh, Jharkhand, M.adhya Pradesh, Maharashtra, Odisha and Uttar Pradesh.
- **Road Connectivity Project** for LWE affected areas (RRP-II) for further improving road connectivity in 44 districts of 9 LWE affected States.
- **LWE Mobile Tower Project** to improve mobile connectivity in the LWE areas.
- The Union Ministry of Home Affairs (MHA) has been implementing the '**National Policy and Action Plan**' since 2015 to combat Left Wing Extremism (LWE).
- The significant features of the new policy were zero tolerance towards violence coupled with a big push to developmental activities so that benefits of development reached the poor and vulnerable in the affected areas.

The Conference of Chief Ministers of the affected states held in Delhi on May 9, 2017 came up with a new formula of **SAMADHAN** to tackle the problem.

- **S** standing for smart leadership,
- **A** for aggressive strategy,
- **M** for motivation and training,
- **A** for actionable intelligence,
- **D** for dashboard-based key performance indicators and key result areas
- **H** for harnessing technology,
- **A** for action plan for each theatre and
- **N** for no access to financing.

2.LEFT WING EXTREMISM OR NAXALISM

What is Naxalism or Left Wing Extremism (LWE):

The term 'Naxal' derives its name from the village Naxalbari of district Darjeeling in West Bengal, where the movement originated in 1967 under the leadership of Charu Majumdar and Kanu Sanyal.

It refers to the use of violence to destabilize the state through various communist guerrilla groups.

Philosophical background of Naxalism:

Naxalism in India, like any other leftist movement around the globe draws its ideological basis from the **Russian revolution** wherein Lenin successfully fought against the Czar through a combination of peasant movement and an armed struggle. The prime intent was to bestow power in the hands of the exploited and marginalized and enforce societal control over governance and nation building.

After the success of the Lenin-led revolution in Russia, the intellectual class in many countries started thinking of ushering in a change in their respective nations. Prominent amongst them were **Fidel Castro** and **Mao Zedong**.

In China, **Mao Zedong** used this philosophy successfully which led to the origin of 'Maoism'. Maoism is a doctrine that teaches to capture State power through a combination of armed insurgency, mass mobilisation and strategic alliances. Mao called this process, the 'Protracted People's War'. **'Political power grows out of the barrel of a gun'** is the key slogan of the Maoists.

Naxalites are far-left radical communists who derive their political ideology from the teachings of Mao Zedong.

History and evolution of Naxalism in India:

Background (The run-up to the Naxalbari uprising):

Tebhaga movement: It was the first communist movement which started in West Bengal in 1946 with the intention of getting the land revenue reduced from ½ to

$1/3^{rd}$. This movement turned violent as the farmers started an armed fight against the landlords.

Telangana Movement: Telangana movement which was led by the people of Telangana in the period of 1946-51 against the atrocities of the Nizam rule also acquired radical dimensions as it progressed.

1959: Kisan Sabhas were started by CPI (Communist Party of India) as an informal peasant movement with the intention of finding a political solution to the problems faced by farmers.

1962: When Indo-China war broke out, majority of CPI leaders viewed it as struggle of a socialist country against Capitalist India. Consequently, they supported China's cause, and faced mass arrests.

1964: Further, there was growing dissent in party for party's diversion toward democratic state which was contrary to Communist principle of armed struggle to overthrow the state. This finally led to a split in the party in 1964 which resulted in new party called Communist Party of India (Marxist).

1967: CPI (Marxist) participated in polls and formed a coalition United Front government in West Bengal. This leads to schism in the party with younger cadres, including the "visionary" Charu Majumdar, accusing CPM of betraying the revolution.

Naxalbari Uprising (25th May,1967): The rebel cadres led by Charu Majumdar launched a peasants' uprising at Naxalbari in Darjeeling district of West Bengal.

The CPI (M)-led United Front government cracked down on the uprising and in 72 days of the rebellion, a police sub-inspector and nine tribals were killed. The incident echoed throughout India and naxalism was born.

The spread and growth of Naxalism in India can be broadly divided into three phases or stages as described below:

The first phase of Naxalism:

In response to the crackdown by the Government, revolutionary leaders fled the area and declared armed struggle against state of India. Under the leadership of Charu Majumdar, they formed a new party **Communist Party of India (Marxist-**

Leninist) in 1969 which was motivated and influenced deeply by Communist Party of China.

After Charu Majumdar's death, the CPI (M-L) was deprived of any credible central leadership and the party withered away to be finally reborn as CPI (M-L) Liberation in 1974.

The movement faced a severe blow during emergency when around 40,000 cadres were imprisoned in 1975.

The Second Phase of Naxalism [Steady growth of the Naxal movement across different parts of the country]:

The movement arose again in a more violent form after the emergency. It continued to widen its base as per the strategy of 'protracted war'. Their base grew from West Bengal to Bihar to Odisha and also to Andhra Pradesh and Chhattisgarh.

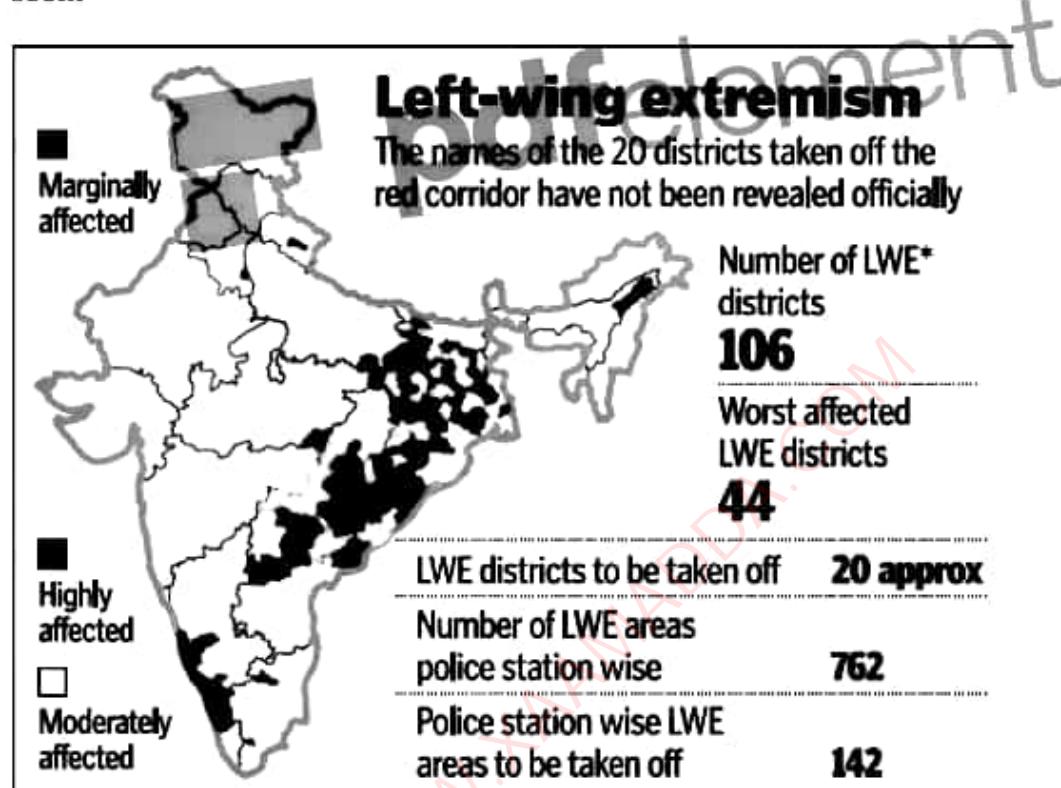
CPI(ML) was converted into People's War Group (PWG) in 1980 which had its base in Andhra Pradesh and struck heavy casualities among police personnel.

Simultaneously, Maoist Communist Centre of India (MCCI) grew in strength in Bihar and carried out large scale attacks on landlords and other upper caste outfits.

The Third Phase of Naxalism:

2004: Andhra Pradesh's PWG and Bihar's MCCI merged to form CPI(Maoist). CPI (Maoist) is the major Left Wing Extremist outfit responsible for most incidents of violence and killing of civilians and security forces. It has been included in the Schedule of Terrorist organisations under the Unlawful Activities Prevention Act, 1967.Over 13 LWE groups are currently operating in the country.

The movement's capacity to challenge the state has increased enormously considering the incidents of violence and casualities resulting from them. E.g. the 2010 Dantewada ambush in which 76 CRPF armed personnel were killed.

2013: The LWE movement made international headlines when naxalists killed 27 people, including some high level politicians, in Sukma district of Chhattisgarh.

But violence cannot be the only yardstick to measure Maoist expansion. Maoists are also expanding in terms of indoctrination and consolidation. They are also trying to

spread their ideology in the Bhil and Gond tribes dominated area, the 'golden corridor' stretching from Pune to Ahmedabad.

As of **February 2016**, 106 districts in 10 States have been identified by the Government of India as Left Wing Extremism (LWE) affected districts in the country.

Estimated to be 40,000 strong, the Naxalites have been a strain on the country's security forces and a barrier to development in the vast mineral rich region in Eastern India known as the 'red corridor'. It is a narrow but contiguous strip passing through Jharkhand, Chhattisgarh and Odisha.

July 2016: The Union government plans to reduce the number of Maoist-affected districts by about a fifth. This decision has been taken on the basis of the districts' violence profile, an assessment of the kind of logistical and other support provided to armed Maoist cadres by their sympathisers and "over ground workers", and the kind of positive changes brought about by development work that these districts have seen.

Most of the worst affected districts fall in the Dandarkaranya region which includes areas of Chhattisgarh, Odisha, Maharashtra and Andhra Pradesh. Maoists have been running a parallel government and a parallel judiciary in these regions.

Ideology and objectives of Naxalites:

From their ideology, it appears that naxalites are fighting for the rights of the poor and want to establish a people's government, but the facts are quite contrary. Social uplifting of the downtrodden is not their real aim, rather it is political power.

They study the local problems and issues and use them as fodder to foster their end game which is clearly the seizure of power through violent means.

Maoists have vested interest in keeping poverty alive because it enables them to expand their territory. They don't allow district administration to do any development work like building roads, improving electricity and water supply in these areas etc.

Modus Operandi

- **Frontal Organisations of LWE**

The Maoists use their front organisations like Revolutionary Democratic Front, Democratic Student Union etc to generate people's sympathy through persistent pursuance of propaganda on issues like human rights violations by the security forces.

- **Guerrilla warfare tactics**
- Powerful **propaganda machinery** which is active in all major towns as well as in the national capital. They even have their supporters in the media.
- **Tactical Counter Offensive Campaign (TCOC):**

Maoists carry out violent activities called TCOC which run from March to early Monsoon in July. The Maoists usually resort to TCOC every year to put the security forces in disarray so that they can go on a recruitment drive.

- Fresh strategy of Maoists is to expand outside forests into the **urban areas** to win over non peasant classes and other social groups.
- The Maoists have also maimed and murdered those they suspect of being '**informers**'.

Sources of funding and linkages with organized crime:

The main source of funding of the LWE movements is **extortion** from government projects as well as from corporate companies working in their areas of influence. Most of the time, it is in the form of **protection money**. LWE is most intense precisely in areas which are rich in mineral resources. It therefore provides them enough scope for extortion.

Sometimes, they also resort to **kidnapping and killings** to terrorise and extort money.

Factors responsible for the rise and spread of LWE:

1. India's Land Reform Policy

Post independence, the land reform policy of India could not be successful in some parts of the nation, leading to the birth and growth of naxal movement in India.

2. Development Projects and Tribal Alienation

The tribals are driven by grievances with the Indian Government over decades long resource mismanagement and systematic marginalisation beginning with a series of development projects in the 1980s that removed tribals from their lands in the name of public good. The conflict between economic progress and aboriginal land rights continues to fuel the Naxalite's activities.

Arundhati Roy, a Naxalite sympathiser said that the tribal forestlands should be called a "MoUist Corridor" instead of the "Maoist Corridor" as the people of these tribal forest lands have been wrestling with "memorandum of Understanding" (MoUs) of the mining companies.

The sociologist Walter Fernandes estimates that about 40% of all those displaced by government projects are of tribal origin.

3. Forest Protection Act of 1980

Although the legislation was an attempt to protect country's natural resources from exploitation, the law essentially outlawed the existence of many tribal villages that had been in place for centuries. As areas were delineated as reserve forests, traditional occupations of even gathering twigs were forbidden. People who earned their livelihood through access to forest resources in a sustainable manner suddenly found themselves outside the law.

It was only in 2008 that amendment to forest rights act recognised the tribals' rights over forest land and forest produce but animosity towards the government had already grown substantially exacerbated by the lack of basic development support to tribal villages.

4. Developmental Deficit and economic inequality

Tribal poverty today is worse than that of Scheduled castes and on par with those of sub-Saharan African countries.The districts that comprise the red corridor are among the poorest in the country.

A key characteristic of this region is non diversified economic activity solely dependent on primary sector. The region has significant natural resources, including mineral, forestry and potential hydroelectric generation capacity E.g. Chhattisgarh, Andhra Pradesh, Odisha, and Jharkhand account for approximately 85% of India's coal resources. Exploitation of the natural resources for the economic progress of the country, ironically, has led to displacement and deprivation of the tribals, further leading to a feeling of alienation.

5. Social Conditions:

The area encompassed by the red corridor tends to have stratified societies, with caste and feudal divisions and violence associated with friction between different social groups.

6. The governance deficit:

- Lack of education facilities and basic sustainable employment

- Lack of basic healthcare facilities
- Infrastructure deficit
- Issues related to law and order, grievance redressal
- Lack of routine administration and poorly motivated public personnel
- Mismanagement and corruption in government schemes like Public Distribution System.
- Poor implementation of special laws
- High handedness of the local administration

7. Geographical factors:

The terrain in these areas is suitable for guerrilla tactics.

It is also because of the terrain that the reach and spread of governmental programmes has been slower in these areas. In these remote upland areas, public officials are unwilling to work hard, and often unwilling to work at all and these postings are often termed as 'punishment postings'. On the other hand, the Maoists are prepared to walk miles to hold a village meeting, and listen sympathetically to tribal grievances.

The Maoists live among, and in the same state of penury as, the tribals. Also, some of their actions have sometimes helped the adivasis. This is especially the case with rates for the collection of non-timber forest produce, such as tendu patta, which have gone up by as much 200% in areas where the Naxalites are active and the contractors fearful of their wrath.

8. Inability of the tribal leaders to get their grievances addressed by the formal political system.

Naxalite movement: the biggest internal security threat to India:

Former Prime Minister Manmohan Singh described Naxalism as the most significant threat to internal security being faced by the country. This proposition is true as it highlights India's interior weaknesses, which make India vulnerable to external threats. It affects several areas including the economy, security and foreign affairs, its citizens and the rule of law:

1. Impact on security and foreign affairs: Links with other terrorist organisations and foreign countries:

The CPI(Maoist) has frequently expressed solidarity with the Jammu and Kashmir terrorist groups and north-east insurgent groups. The CPI(Maoist) has also had close links with foreign Maoist organisations like Turkey, Phillipines,South asian countries etc.

2. Impact on economy: More the Maoists concentrate in the poor and marginalised regions of India, the more the economic development (which is imperative to improving these regions) will be hampered. The Naxalite activities are using up scarce resources on defence and internal security when it should be spent on areas such as social development.

3. Impact on citizens and the rule of law: Not only has there been a great loss of life since the conflict between the guerrillas and the military, but addressing the problem through violence risks polarizing people further and driving them to subservience.

Guerrilla warfare is a threat not only to citizens' lives but also to their property. Too impatient and desperate to wait for government intervention, civilians such as landlords are taking matters into their own hands.

As writer Navlakha noted , by portraying the Maoists as a 'menace' and separating the movement from socio-economic causes, it "allows the rich and poor divide to impose itself on a formal democratic structure". Navlakha gives the example of Bihar where Naxalite groups are banned under the Prevention of Terrorist Activities Act, yet a majority of the massacre were committed by landlord armies which were

not considered an act of terror under the law. Such treatment for the upper class only serves to threaten the rule of law, state legitimacy and democracy as the political norm.

Challenges in dealing with Naxalites:

1. Expansion in adjoining areas due to hard combat:

Hard combat against the Naxals pushes them out temporarily but they use other states to regroup and rearm. This can be associated with the Andhra Pradesh model, where the intensive use of Greyhounds had led to a lot of spillover to other states.

2. Expansion due to increasing association with Anti-state forces:

New territory in new states may result in a corridor for Naxals to collaborate with other insurgent groups who are essentially ideologically different but are anti-state. There has been increasing collaboration between the naxals and the pro-Azadi leaders in J&K and ULFA training the naxal cadres.

3. Expansion of Naxal activities due to international collaboration:

The likely collaboration with international maoist movements, may give it a much more dangerous dimension, to tackle which India seems to be unprepared. There is also an increasing threat of rising terror outfits' support to the naxal operations in India.

4. Administrative hurdles in dealing with LWE:

- Poor infrastructure, lack of communication and shortage of manpower
- A virtual parallel government run by Maoists in Dandakaranya region
- Poor coordination among various state police forces
- Lack of proper understanding between the central and state forces

5. Intellectual support to naxalism:

Top intellectuals like Arundhati Roy and Binayak Sen regularly support naxalism, advocating an egalitarian society, human rights and tribal rights. But use of violent

means cannot be supported to achieve a noble cause in a democratic setup. Rather than a blind support, the intellectuals should also encourage Naxals to eschew violence, fight elections, join mainstream society and learn the art of give and take of democratic bargaining without aggression.

The Government's strategy to address Left Wing Extremism (LWE)

1. Ban on CPI Maoist, along with all its formations and front organizations under the Unlawful Activities (Prevention) Act, 1967.

2. Assistance to LWE States: 'Police' and 'Public order' being State subjects, action with respect to maintenance of law and order lies primarily in the domain of the concerned State Governments. However, the Central Government closely monitors the situation and coordinates and supplements their efforts in several ways to deal with the LWE problem. These include:

- providing Central Armed Police Forces (**CAPFs**) and Commando Battalions for Resolute Action (**CoBRA**),
- setting up of Counter Insurgency and Anti Terrorism (**CIAT**) schools;
- **modernization** of the State Police and their Intelligence apparatus etc.

Assistance is also provided by the central government under the following schemes:

- Security Related Expenditure Scheme (**SRE**)
- Special Infrastructure Scheme (**SIS**)
- Central Scheme for assistance to **civilian victims**/family of victims of terrorist, communal and naxal violence
- Civic Action Programme (**CAPs**)

3. Action Plan: The Government has formulated National Policy and Action Plan adopting **four pronged strategy** in the areas of security, development, ensuring rights & entitlement of local communities and management of public perception.

4. Strengthening the **intelligence mechanism**: This includes intelligence sharing through Multi-Agency Centre (MAC) at the central level and State Multi Agency Centre (SMAC) at the subsidiary level on 24×7 basis.

5. Better inter-state coordination by way of frequent meetings and interaction between the bordering districts of LWE affected states.

6. Media plan: The media has proved to be a potent instrument in creating awareness among the target population about the socio-economic developmental schemes of the Government and their rights & entitlements. The media has also helped to highlight LWE activities to make people aware as to how LWE violence is preventing implementation of the welfare and development schemes, policies and initiatives of the Government.

7. A Surrender and Rehabilitation Policy for LWE cadre surrenderees.

8. Roshani Scheme (Ministry of Rural Development): It is a placement linked skill development scheme for rural and tribal population in worst affected districts. It emphasizes on special efforts to proactively cover the particularly vulnerable tribal groups (PVTGs) on a priority basis.

A few success stories in the fight against Naxalism

Sandesh(Bihar)

Sandesh block in Bihar has seen a gradual elimination of Naxalites. The most important factor which proved instrumental in dismantling naxal dominance was the panchayat elections initiated in Bihar. It created a significant distance between the Naxal leaders and the local community. Social pressure forced many naxalites to switch over to farming and shed off their association with naxal outfits.

Aasdwar project in Jehanabad (Bihar)

Under this project, 5 Naxalite affected panchayats (Jehanabad district of Bihar) are witnessing a flurry of development activities on a war footing e.g. construction of cement lanes, link roads, drains, buildings for schools and anganwadis, individual toilets etc. The people, at large, seem to have embraced the programme in a big way.

So, as this case study amplifies, Naxalism can be defeated and eliminated by the process of development and a new social order but the change has to come from within.

AP greyhounds model

Andhra Pradesh's Greyhound naxal fighting force along with infrastructure development and effective surrender and rehabilitation policy has also proved effective. Other elements in the Andhra Pradesh model include:

- Culture of police leadership
- Sound knowledge of local terrain
- Incentives to police for good work
- Operations based on local intelligence
- Grass roots involvement in anti-Naxal operations

The way forward:

Naxalism is not merely a law and order issue. To truly eliminate naxalism, we must undercut its raison d'être, its reason for existence. While the methods of Naxalites may be abhorrent, most of their goals (apart from overthrowing the government) are not. The government must fulfill these goals for them so that they have nothing to fight for.

The government must adopt a multipronged composite strategy. We can broadly divide the strategy as follows:

1. Development strategy:

- Better infrastructure in core naxal areas
- Special forcus on political security and accelerated socio economic development in a holistic manner
- Political parties must strengthen their cadre base in naxal areas
- Decentralisation and participative democracy

- Better implementation of government schemes

2. Security strategy

- Promote local resistance groups on lines on 'village defence committees' in J&K
- Formation of specially trained special task forces on the pattern of Greyhounds in affected states
- Professional dominance by security forces with primacy of state police at all levels
- Modernisation and upgradation of state police infrastructure, weapons and technical equipment
- Strengthening local intelligence units
- Tightening control on availability of explosives
- Posting of competent and motivated police officers in LWE affected areas

3. Psychological Operations

- Administration should engage with public at large, civil society, NGOs to restore people's faith and confidence in the government machinery
- Media and public perception management

4. Other measures

- The doors for peace talks should always be open
- There should be genuine attempts to win the hearts and minds of people
- Time-bound conviction of arrested cadre must be ensured through vital reforms in criminal justice system
- Effective surrender and rehabilitation policy ensuring proper safety and care of their families
- Better adherence to law legislated for protection and development of tribals

5. Understanding the tribal psychology and addressing their concerns:

Efforts should be made to better understand the tribal psychology e.g. the tribals having been left out of the development process are also oblivious to the potential enhancement in the quality of life if the growth process were to touch them. If they knew the potential benefits of growth, they would realize the futility of violence and see reason to participate in the growth process and become part of the mainstream without losing their identity and culture.

Another example:The tribals' opposition to part away with their land is not only due to livelihood concerns, but also their shield against a system they are unfamiliar with. The fear of not being fit enough to participate in a system alien to them also adds as a disincentive to give up their land. This, in the end, results in a conflict as there is a clash of ideas that ultimately drives the tribals further away from the mainstream and the reach of the Indian State.

Efforts should therefore be made to better understand the tribal psychology and address their concerns.

6. Need for policy changes:

Nanadan Nilekani in his book 'Imagining India' argues that empowering local tribal communities to take decisions on forest resources and environment through PESA and the Forest Rights Act can enable them to leverage their lands for economic gains. Nilekani argues that the challenges posed by climate change have actually opened up the possibility of integrating the unorganized economic activity of the tribals. He adds that once resource rights are established, rural and tribal communities can earn incomes by participating in carbon cap and trading schemes with businesses and industries. Connecting these tribal groups (in the same way NCDEX has connected India's farmers to commodity markets) would bring these communities into our markets in big way.

But, measures such as these require drastic policy shifts at the very top. An environment policy for the future could indirectly bring the historically marginalized citizens of India i.e. the tribals into the mainstream facilitating participation in the larger growth process of an economically resurgent India

3. THE NORTH-EAST INSURGENCY

The North-East region:

The Northeast region of India comprises eight states – the Himalayan state of Sikkim and the contiguous seven Sister States (Arunachal Pradesh, Assam, Manipur, Meghalaya, Mizoram, Nagaland, and Tripura).

North East India is connected to the Indian mainland by a small corridor – Silghuri Corridor (also known as **Chicken Neck** – with a narrow width of only 23 kilometers.)

Strategic Importance of the region: About 99% of the 6387 km border of this Region is international border along Bangladesh, Myanmar, China and Bhutan. It

makes up close to 40% of India's land borders with its neighbours. It thus has an extraordinarily important international strategic dimension and is a vital part of the nation's defence architecture.

Bridge to South East Asia: The region is a bridgehead between India and the vibrant economies of Southeast Asia, including southern China.

Economic Significance: North East is endowed with huge natural resources (oil, gas, coal, hydro, fertile land, etc) which can be harnessed for nation development.

A historical background of the North-East

Pre-independence era: During the British era, the tribal groups constituted an overwhelming majority of the population in most of the areas they inhabited. Outsiders were not allowed to acquire land in the tribal areas. At the same time, the British government supported the Christian missionaries to move in and establish schools, hospitals and churches.

There was a virtual absence of any political, cultural, social, geographical, religious or business contact of the tribals in the North-East with the rest of the India. So India's freedom struggle had very little impact on the tribals.

Post-independence era: The sixth schedule of the Indian Constitution provided for self rule, autonomy and decentralisation in the region. Thus district and regional councils were created.

Initially, there was only one state of Assam and one Union Territory NEFA (North East Frontier Agency) covering the whole of north-east.

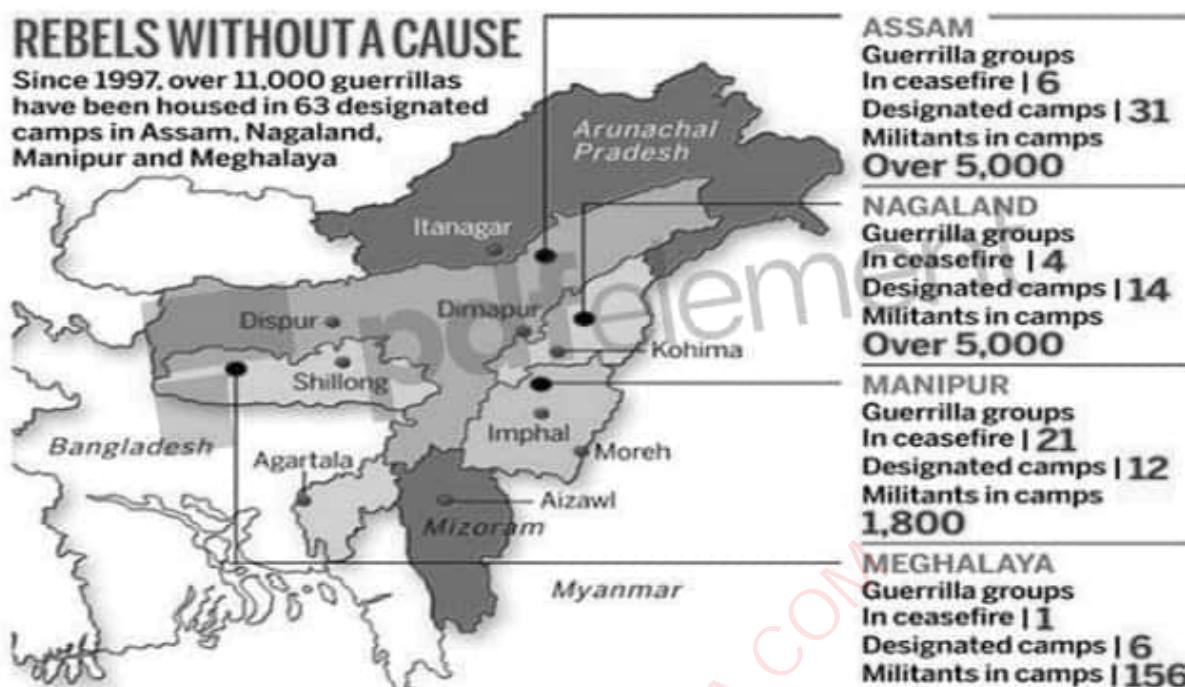
While NEFA was developing comfortably and in harmony with the rest of the country, problems developed in other tribal areas which were a part of Assam administratively. The tribals were afraid of losing their identity and being assimilated by the policy of Assamization in government jobs and other professions.

There were demonstrations and a major agitation developed. In 1969, Meghalaya was carved out of Assam as a 'state within a state'. Finally, Meghalaya, Manipur, and Tripura were granted statehood in 1972.

Meanwhile, secessionist movements developed in Nagaland and Mizoram. Nagaland was granted statehood in 1963 itself, while Mizoram became a state in 1987. Also, NEFA was renamed as Arunachal Pradesh and granted the status of a separate state in 1987

Difference between insurgency, terrorism, militancy and extremism

Before we move further, it is important to understand the difference between the terms 'insurgency', 'terrorism', 'militancy' and 'extremism'.

Militancy is a condition which experiences the use of violence, being combative or predisposed to fight. Militants can include any individual or group which takes to violence. This need not only **include terrorists and insurgents**, but also religious groups which take to violence to further their beliefs.

Extremism is a state wherein a person or an organisation holds extreme political or religious views.

If one were to compare these terms, an extremist may not necessarily be committing a crime under the law. A number of groups, political and religious, fall under this category, for instance, the separatists in Kashmir and Maoist supporters.

Insurgency: The Indian Sub Conventional Doctrine defines **insurgency** as "an organised armed struggle by a **section of the population** against the state, usually with foreign support. Possible causes of an insurgency including ideological, ethnic or linguistic differences; or politico-socio-economic reasons and/or fundamentalism and extremism."

An insurgency may have within its fold both militant groups supporting it as also extremists who propagate its ideology. But, insurgents are our own citizens, whereas terrorists may not always be our own citizens.

Present Situation of insurgency in the North-East

The security situation in some of the north-eastern states has remained complex for a long time because of a number of militant outfits and their diverse demands. Assam, Manipur and Nagaland have continuously been a point of worry.

The Government has steadily followed a policy of dialogue and negotiations with any outfit which agrees to forego the path of violence and come forward for peace talks within the constitutional framework of India. In general, the security situation in most of the north-eastern states has shown considerable improvement during the last 5 years.

Major Insurgent Groups operating in North Eastern States

ASSAM	
(i)	United Liberation Front of Assam (ULFA)
(ii)	National Democratic Front of Bodoland (NDFB)
(iii)	Kamtapur Liberation Organisations (KLO)***
MANIPUR	
(i)	People's Liberation Army(PLA)
(ii)	United National Liberation Front(UNLF)
(iii)	Peoples' Revolutionary Party of Kangleipak (PREPAK)
(iv)	Kangleipak Communist Party (KCP)
(v)	KangleiYaolKannaLup (KYKL)
(vi)	Manipur Peoples' Liberation Front (MPLF) and
(vii)	Revolutionary Peoples' Front (RPF) and
(viii)	Coordination Committee Cor-com (conglomerate of six valley base UG outfits).

MEGHALAYA	
(i)	Hynniewtrep National Liberation Council (HNLC)
(ii)	Garo National Liberation Army (GNLA) ***
TRIPURA	
(i)	All Tripura Tiger Force (ATTF)
(ii)	National Liberation Front of Tripura (NLFT)
NAGALAND	
(i)	The National Socialist Council of Nagaland (IsakMuivah) - [NSCN(I/M)]
(ii)	The National Socialist Council of Nagaland (Khaplang) [NSCN (K)]**
(iii)	The National Socialist Council of Nagaland (Khole-Kitovi)[NSCN(KK)]
(iv)	The National Socialist Council of Nagaland (Reformation)[NSCN(R)]
* All the militant outfits mentioned above except NSCN/IM, NSCN/KK and NSCN/R, have been declared 'Unlawful Associations' under the Unlawful Activities (Prevention) Act, 1967. In addition, the outfits named above in respect of Assam, Manipur and Tripura have also been listed as 'terrorist organizations' in the schedule to the above Act. ** NSCN/K declared as 'Unlawful Association' & terrorist organisation. *** KLO and GNLA declared only as a 'terrorist organizations'.	

State wise status and reasons behind the insurgency:

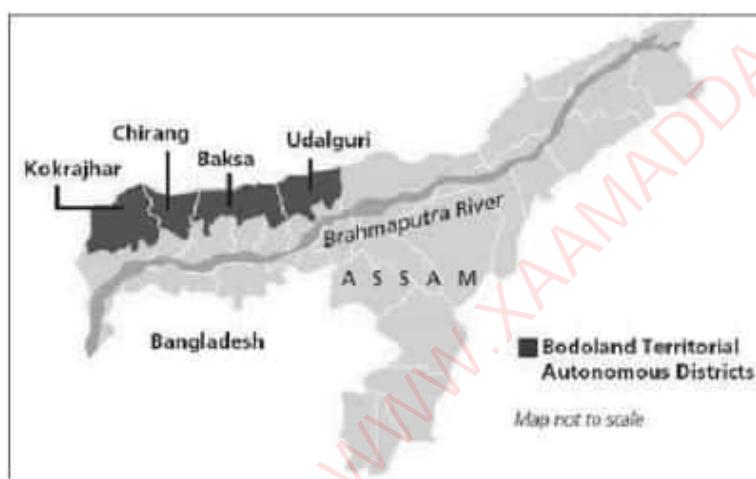
Nagaland:

The Nagas believe that they were not part of India, whether through conquest or consent. The Nationalist Socialist Council of Nagaland (NSCN) is a Naga nationalist group operating in North-east India. The main aim of the organisation is to establish a soverign state, "Nagalim" unifying all the areas inhabited by the Naga people in Northeast India and Burma

Issues:

- Clashes among different tribal groups and factions

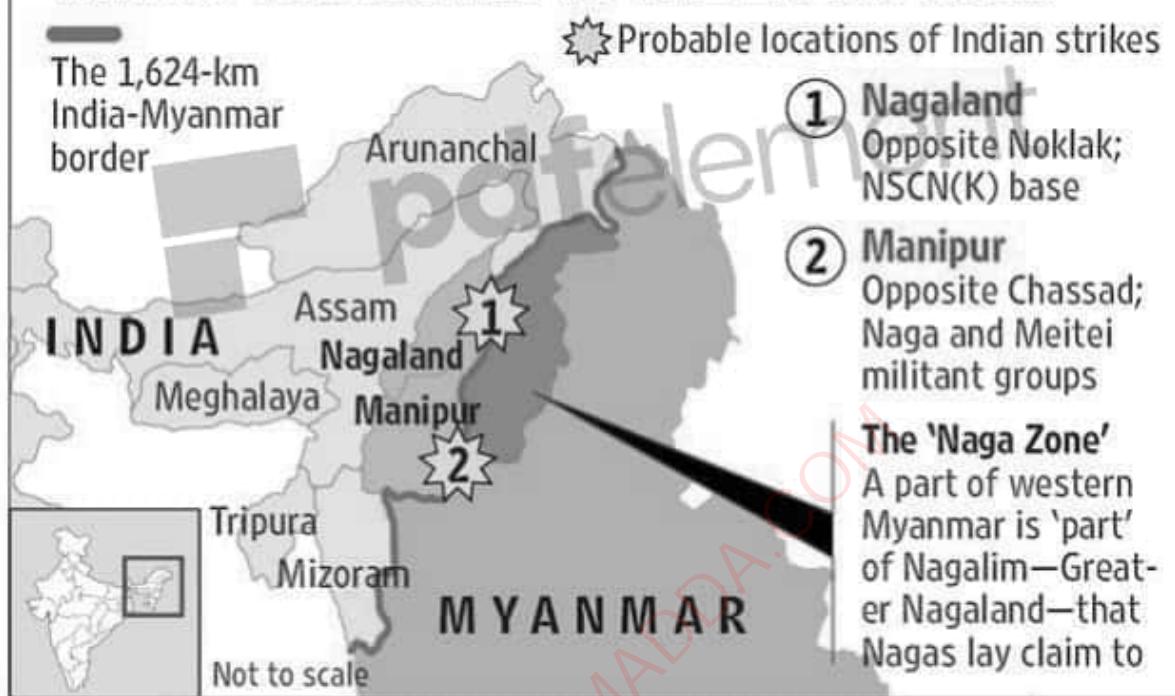
- Presence of underground groups that deal in extortion, arms, drugs, smuggling etc.
- Parallel government

Recent developments:

The govt of India and Naga insurgent group NSCN (IM) signed a peace accord on 3 August 2016. However, this is only a framework agreement. The details of the accord are yet to be fleshed out. It is likely to be followed by more detailed agreements and negotiations.

Assam:

The perceived threat to the political identity of the Assamese people from the illegal migrants from Bangladesh lies at the core of the Assam problem. The indigenous people of Assam feel that in future the illegal migrants will become the majority population and they will lose political power.

Statehood demands in Assam:

1. Bodoland
2. Karbi Anglong
3. Dimaraji
4. Kamtapur

Recent developments:

In July 2012, violence broke out with riots between indigenous Bodos and Bengali-speaking Muslims (who were suspected to be illegal Bangladeshi muslims). Violence in Assam later had its repercussions in other parts of India, Azad maidan riots in Mumbai, Rumour mongering (via sinisterSMSs) triggered exodus of NE Indians

Manipur

The people of Manipur include the Meitei tribe, the Kuki tribe and the Naga tribe. Meitei tribe forms about 60% of the total population and lives in the plains while Nagas and Kukis live in the hill districts.

Issues:

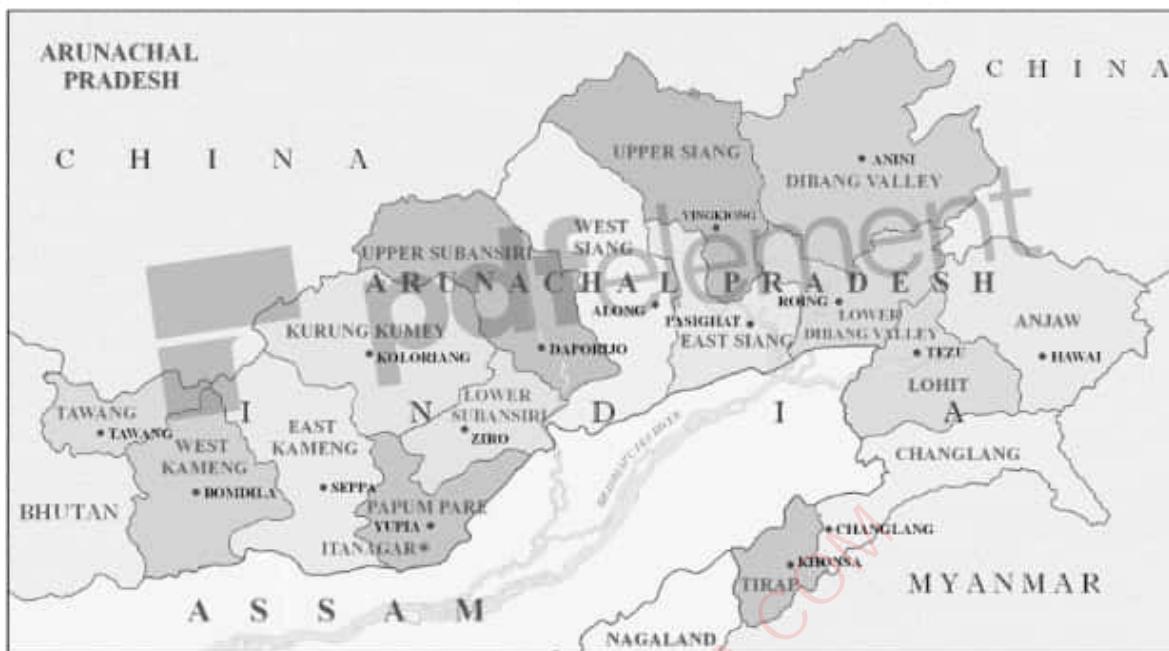
- There are more militant groups in the states than anywhere else and the rivalry between these outfits often leads to greater violence.

- The situation is further complicated because insurgent groups are not united for the same cause. The Nagas wish to annex a part of Manipur and merge with a greater Nagaland or Nagalim, which is in conflict with Meitei insurgents' demands for an independent state.
- Unlike other conflict theatres of the Northeast, not many 'surrenders' have been reported from Manipur, thus indicating the tight control that the outfits have maintained over their cadres.
- Also, non-Manipuris are being targeted increasingly in Manipur.

Recent developments:

In June 2015, 18 Indian Army jawans were killed and several others were injured when suspected militants ambushed their convoy in Manipur's Chandel district. In response to the killing of 18 of its troops by militants in Manipur, the Indian Army in one of its biggest covert missions sent troops into Myanmar to strike at two camps and, according to official estimates, killed over 20 suspected militants.

Meghalaya

Meghalaya is perhaps the least affected by insurgency in the north-east region.

Problems in Meghalaya arise from the divide among various tribes as well as the divide between tribal and non tribal settlers, identity issues and growing corruption, besides the sharp changes in demography due to Bangladeshi infiltrators. Also,

criminal activities like extortion and drugs smuggling are a major concern in the region. The state lies in a major smuggling route between Bangladesh and India.

Mizoram and **Tripura** have shown remarkable success in controlling insurgency and now they are largely peaceful.

Arunachal Pradesh

The people of three eastern districts of Arunachal Pradesh, namely Tirap, Changlang and Longding live in perpetual fear due to presence of cadres of two NSCN factions in the area, who resort to kidnapping, extortion and factional feuds. These three districts are a part of NSCN-IM's projected state of Nagalim (Greater Nagaland).

Arunachal Pradesh has also been used as atransit rout by the ULFA (United Liberation Front of Asom).

MIZORAM:

A situation **similar** to Nagaland developed a few years later in autonomous Mizo district of the Northeast. Sessionist demand backed by some British officials had grown there in 147 but had failed to get mush support from the youthful population.However, unhappiness with the Assam government's relief measure

during famine of 1959 and the passage of the Act in 1961, making Assamese the official language of the state,led to the formation of Mizo National Front (MNF),with Laldenga as president.

While participating in the elections MNF created a military wing which received arms and ammunition and military support from East Pakistan and China. In March 1966 MNF declared independence from India, proclaimed a military uprising. The GOI responded with immediate massive counter insurgency measures by the army. Within a few weeks insurgency was crushed and government control was restored.

In 1973, after the less extremist Mizo leaders has scaled down their demand to that of a separate state of Mizoram within the Indian Union, Mizo district of Assam was separated from Assam and, as Mizoram was given the status of a Union Territory.

Mizo insurgency gained some renewed strength in the late 1970's but was again effectively dealt with the Indian armed forces.

A settlement was finally reached in 1986.An 'accord' was signed between the Union Government and the Mizo National Front in 1986 ,according to which insurgents group agreed to surrender before the Union and re-enter the constitutional political

stream. A year later, statehood was conferred. Since the MNF has a formidable political force in the state.

Hmar insurgency

Not satisfied with the Mizo Accord of 1986 that ended two decades of insurgency led by the Mizo National Front (the peace deal did not grant the Hmar tribe administrative autonomy), some Hmar leaders formed the Hmar People's Convention (HPC), and began a struggle for autonomy. The insurgency raged until 1994, when the Mizoram government set up the Sinlung Hills Development Council for Hmar-inhabited areas. The HPC joined the political mainstream, but Mizoram police and politicians say their best weapons were never surrendered, and an offshoot — the Hmar People's Convention Democrats (HPCD) — emerged almost immediately and pressed on with the old demands.

Who are Hmar?

They are a tribal people living in Assam, Mizoram and Manipur, mainly in the area where these states meet. Although the Hmar identity is strong, Mizos in general consider them as part of the community, or at least as one of tribes that make up the Zohnahthlak, a loose grouping of tribes with largely similar customs, dialects and dress who live in Mizoram or its immediate vicinity. Many Hmars are members of Mizoram's middle class; most no longer speak the Hmar dialect, and are fully integrated into Mizo society. In Manipur, the tribe is sometimes loosely included in the Kuki group, evidenced from the fact that one of the main Hmar armed groups — the HPCD — is considered part of the "Kuki armed groups" (more specifically, the United People's Front group of **militants).**

Demands of the Hmar Insurgents:

The HPCD's stated demand is a separate tribal autonomous district, and sometimes a state called Hmar Ram, for the Hmar tribe.

It suffers from two main weaknesses:

1. The outfit is largely based in Manipur and a corner of southern Assam and has only thin physical presence in Mizoram

2. There are two HPCD factions

Factors responsible for insurgency in the Northeast

- Lack of development and basic amenities coupled with corruption and diversion of funds, often to the coffers of insurgents e.g. siphoning of food-grains meant for the public distribution system, a large proportion of which falls in the hands of the militants
- Unemployment problem in the region stands as a major cause for sustained insurgency.
- Feeling of alienation and deprivation among the tribal population
- Demography: In spite of several political permutations and combinations, the political boundaries in most cases do not coincide with the existing social boundaries. It has lead to the demands of various ethnic categories for recognition of their distinctive identity.
- Similar ethnicity across the border on Myanmar side
- Porosity of the border with Myanmar due to difficult terrain
- Change in demographic pattern due to infiltration from across the border
- Disconnect with the other parts of India and fellow Indians
- Widespread corruption among the ruling elite
- Lack of visionary leadership among the tribal communities
- Easy availability of arms and ammunition
- Political support from various factions
- Instability in Myanmar
- Factional in-Fighting among the insurgent groups.
- Military reasons – AFSPA (Armed Forces Special Power Act).
- External support – China and Myanmar.

Challenges and concerns:

1. The linkage with organised crime

The biggest challenge to the North East is extortion carried out by various insurgent groups. Extortion has become meticulously organised activity in the region and is one of the major sources of funds for the militants. Other sources of their funding include arms and drugs smuggling.

2. Maoist Consolidation in North East:

The Maoists have been able to extend the red corridor to the Northeast. The arrests of various top Maoist leaders in this region during 2013 revealed the extent of Maoist infiltration in Northeast India.

The Maoist rebellion in Northeast India is at present in its 'latent phase' which involves mobilization of the masses, political awakening, visiting villages, engaging in small struggles on local issues, picking up students' issues, fighting corruption, short–listing shelter and arms dumps and identification of local militant elements.

3. Spread of Islamist Militancy:

Northeast India, shares an 1880 km long porous border with Bangladesh, a country that is a hotbed of Islamist militancy. Though radical Islam has not yet seeped into

the Muslim population in the region, the arrests of twelve persons in Assam during November-December 2014 with links with the Islamist terror outfit Jamaat-ul-Mujahideen Bangladesh (JMB) shows that radicalization of a section of Muslim population has begun in the region.

4. Trans-national linkages

India's Northeast is one of South Asia's hottest trouble spots, not simply because the region has as many as 30 armed insurgent organizations operating and fighting the Indian state, but because trans-border linkages that these groups have, and strategic alliances among them, have acted as force multipliers and have made the conflict dynamics all the more intricate.

The impact of insurgency on economy:

The persistent insurgency atmosphere has been the most important contributor to economic stagnation of the region.

1. Connectivity:

The gateway to the North Eastern Region is the chicken's neck of Siliguri area in North Bengal and all flows to and from the Region on the surface routes have to pass through this neck and the Brahmaputra Valley of Assam, Guwahati being the grand nodal point. Therefore, any disturbance in the Brahmaputra Valley and/or its adjoining hills brings the activities in the whole of the Region to a stand-still position.

2. Infrastructure:

The subversive activities of the insurgents' damage rail tracks, cause accidents leading to loss of life and property, create terror among the travelers and throw the entire system out of gear. Similarly, vehicles in the State and National highways are often attacked, passengers and transport workers are killed or wounded and sometimes abducted for ransom; and goods are looted.

3. Industry including petroleum and tea:

As the articulated economic grievance hovers around the idea of so called regional colonialism based on the alleged drain of rich resources of the region, any violent political movement makes petroleum and tea as its target.

4. Environment:

On the one hand, insurgents damage forests by taking shelter there and on the other, anti insurgency operations also lead to denudation of forests. This not only means that conservation activities and other forestry operations are hampered thus resulting in the loss of valuable natural resources but also that a grave threat is posed to the fragile ecology of the region.

5. Development of the interior areas

The insurgency has aggravated the problem to such an extent that development workers of both the Government and NGOs are utterly discouraged from going to the hilly and rural areas as they face constant extortion and threats of abduction or death.The insurgents by breeding a cult of hatred against the supposed or real outsiders are blocking all inflows of resources, ideas, expertise and initiative to the societies of the North East.

Government's response

The Central Government is pursuing a policy for talks/negotiation with such groups which categorically abjure violence, lay down arms and seek solutions for their problems peacefully within the framework of the Constitution of India. As a result, number of outfits have come forward for talks with Government and have entered into Suspension of Operation (SoO) agreement, and some of them have signed Memorandum of Settlement (MoS) and yet others have dissolved themselves.

Those who are not in talks are being dealt with by the Central Armed Police Forces and the State Police through Counter-Insurgency Operations.

The Central Government is supplementing efforts of the State Governments in dealing with the insurgency through various measures. These include:

- Deployment of **Central Armed Police Forces** to aid the State authorities for carrying out counter insurgency operations and providing security for vulnerable institutions and installations
- Reimbursement of security related expenditure to the State Governments under **SRE** Scheme. The scheme is being implemented in all States of the region except Mizoram and Sikkim.
- Central assistance to the State Governments for **modernization of State Police Forces**
- Sanction of **India Reserve Battalions** for augmenting and upgrading the states' police forces to deal with insurgency /militancy
- Banning the Unlawful Associations operating in NE Region under **UAPA (Unlawful Activities(Prevention) Act, 1967)**
- Declaring specific areas/states as 'disturbed areas' for the purpose of **AFSPA** and issuing notifications for Unified command Structure etc.
- Scheme for **Surrender-cum Rehabilitation** of militants in North East to wean away the mis-guided youth and hard-core militants who have strayed into the fold of militancy and later find themselves trapped into that net.
- **Civic Action Programme** in the North Eastern States in order to take the local populace in confidence and boost the image of armed forces amongst the common people. Under this Programme, various welfare/developmental activities are undertaken like holding of medical camps, sanitation drives, sports meets, distribution of study material to children, minor repairs of school buildings, roads, bridges, etc. and running adult education centres etc.
- **Advertisement and publicity** to highlight the activities being undertaken by the Government for peace in the region and also with a view to convey that "Peace pays".

Recent Initiatives by the Government for development of the North-East

1. From Look East Policy(LEP) to Act East Policy(AEP):

A greater focus on:

- External Angle : Essentially, concerning relations of India as a whole with ASEAN & East Asia
- Internal Angle : Development of North East India that makes it a viable gate way for the rest of India to ASEAN & East Asia

2. The Kaladan Multi Modal Transit project:

The project will connect Sittwe Port in Myanmar to the India-Myanmar border via roadway. It will provide alternative cost effective shortcut to landlocked north eastern states. Originally, the project was scheduled to be completed by 2014, but work on it is still underway.

Once operational, it will provide an alternate access route to India's north east region and contribute towards the regional economic development and reduce pressure on the Siliguri Corridor.

3. The India-Myanmar-Thailand trilateral highway

The India-Myanmar-Thailand (IMT) trilateral highway is expected to become operational by 2018-19. Also, the Ministry of External Affairs (MEA) is planning to extend the proposed India-Myanmar-Thailand highway to the CLMV (Cambodia, Lao PDR and Vietnam) countries in the second phase. This will then give India direct access to the South-East and East Asian markets

4. Development of Moreh (Manipur) as a smart city:

Manipur is the most critical state in India's connectivity to Myanmar and South East Asia. 99% of overland formal trade goes through Moreh.

5. North East in Hydrocarbon Vision 2030 aims to double oil and gas output in the next 15 years.

6. North East Rural Livelihood Project

It is being implemented in 2 districts in each of 4 North Eastern States of Mizoram, Nagaland, Sikkim and Tripura. The objective is to create sustainable community institutions around women Self Help Groups (SHG), Community development groups (CDG) and the youth of the select districts. It was launched in 2013 for a period of 5 years and is aided by the World Bank.

The way ahead: "Acting East through North East"

Although varying in their demands and methods, there is a common thread running through the insurgency infested north-east, that is of identity and development. Hence, some solutions that are common need to be explored with specifics derived from them for specific regions and groups. Following are some suggestions:

1. Decentralisation with alertness: Meeting the political aspirations of groups by giving them autonomy. Implementing sixth schedule provisions in these areas will help them to preserve their identity and culture while giving them greater autonomy.

2. Need to pursue **a developmental approach**: If institutions of development are created in the region, the problems of politics, society, ethnic strife, militant assertion and of integration will get minimised. E.g.

- Improving road and railway connectivity within the North-East
- Modernization of the primary sector and a vigorous programme of rural development
- Stress on processing industries connected with agriculture, animal husbandry, horticulture and forestry and also service industries related to the rural infrastructure like irrigation, rural electrification, transport and communication, marketing etc.
- Modernization of border trading framework
- Improving infrastructure

Also, the developmental approach must ensure the participation of the masses of all groups in the development process with reasonable equity in the distribution of costs

and benefits. Another point to be stressed is that development in the North East must be ecologically sustainable and must not be eco-degrading.

3. Improving **Governance and delivery mechanisms** of the government and administration.

4. The pre-condition of complete abjuring of violence for holding peace talks is a flawed notion. If violence is discarded and peace is established then the need of peace talks become futile. **Dialogue** should be an ongoing process to reach concrete solutions by involving all the stakeholders and not a single group.

5. Coordinating operations with the **neighboring countries** and use of force only when needed.

6. The report by 2nd ARC recommends that even in dealing with the purely 'law and order aspects' of insurgency and violence in the region, much greater **reliance needs to be placed on the local police** than has been the case so far. While deployment of the Armed Forces of the Union may be required, there is a strong case for minimising their use for operational purposes in a region which still continues to harbour a sense of alienation.

7. State police and central forces should cooperate on **intelligence sharing**, investigation and operations against militants. It has been alleged by the army that the June 2015 ambush of the army became possible because state police did not share the intelligence about the attack with it. It is unfortunate and counter-productive.

8. Also, there is important spill-over effect of insurgency in one State on the contiguous States. Therefore, the problem has to be viewed and tackled in an **integrated manner** considering its regional external effects, uniformity in its basic nature and also the linkage between the insurgent outfits of different States.

9. Civil-military relations are a critical ingredient for a successful political strategy to counter insurgencies in areas like the North East. Better civil-military relations in states like Mizoram ensured that a twenty year old Mizo insurgency (1961-1986) was rooted out through joint civil-military strategies like the grouping of villages,

which had relocated nearly 80 per cent of Mizoram's population to 102 new villages known as 'protected and progressive' villages.

10. Speedy implementation of the **North East Vision 2020** and speedy completion of the projects already underway like The Kaladan Multi Modal Transit project, The India-Myanmar-Thailand trilateral highway etc.

11. The need for **Sub-State diplomacy**: States in border areas have a natural cultural and economic interest in our foreign policy orientation towards our neighbours. There is a need for all the States in North East to be more involved in diplomacy with neighbouring countries. Inclusion of Chief Ministers of Border States of North East in Prime Ministerial visits to neighbouring countries is a welcome step.

12. There is a need to promote a **'pan-India fraternity'** that bridges the psychological and emotional gap between the North-East and the rest of India.

13. A recognition that the security and territorial integrity of India in the North East can be best fortified by the combined economic strength of the States in the North East and their **economic integration** with ASEAN , BIMSTEC and East Asia.

4.JAMMU AND KASHMIR MILITANCY

The ongoing Kashmir Valley unrest needs to be correctly understood and appreciated as a national security issue and challenge. But before we delve into the contemporary issues surrounding Kashmir, it is necessary to briefly revisit history:

A brief timeline:

August 1947: Partition of the Indian subcontinent along religious lines lead to the formation of India and Pakistan.

October 1947 – The Maharaja of Kashmir signed a treaty of accession with India after attacks by a Pakistani tribal army. Under the Instrument of Accession, a temporary special status was granted to the State under article 370 of the Indian Constitution.

1947-48: War broke out between India and Pakistan over the region.

January 1948: India referred the dispute to the United Nations.

August 1948: UN directed Pakistan to remove its troops, after which India was also to withdraw the bulk of its forces. Once this happened, a "free and fair" plebiscite was to be held to allow the Kashmiri people to decide their future. But a plebiscite could not be held, partly because Pakistan would not withdraw its forces from Pakistan-held Kashmir, and partly because Indo-Pak relations got enmeshed in the Cold War.

January 1, 1949: A ceasefire was agreed, with 65% of the territory under Indian control and the remainder with Pakistan. The ceasefire was intended to be temporary but the Line of Control remains the de facto border between the two countries.

1956: The Constituent Assembly of Jammu and Kashmir ratified the accession of the state to India.

1965-66 – A brief war between Indian and Pakistan over Kashmir ends in a ceasefire and signing of the Tashkent agreement.

1971-72 – Another Indo-Pakistani war ended in defeat for Pakistan and the formation of the independent nation of Bangladesh (formerly known as East Pakistan) which lead to the 1972 Simla Agreement. This turned the Kashmir ceasefire line into the Line of Control, and both sides pledged to settle their differences through negotiations.

Start of insurgency

1987 – Disputed state elections in Jammu and Kashmir gave impetus to a pro-independence insurgency. India accused Pakistan of fomenting the insurgency by dispatching fighters across the Line of Control, which Pakistan denied.

1990 – India imposed Armed Forces Special Powers Act (AFSPA) in Jammu and Kashmir following escalation of insurgency.

1990s – Violence intensified in Kashmir. Islamic militants carried out ethnic cleansing in the Kashmir Valley, terrorizing non-Muslims, mainly Kashmiri pundits,

causing large numbers of people to flee, mainly to Jammu. The Indian military responded with repression to the terrorism, foreign infiltration, and the domestic insurgency, which are now all mixed up. There are allegations of serious human rights abuses on all sides.

Recent events:

March 2015 – India's ruling BJP party was sworn into government in Kashmir for the first time in coalition with the local People's Democratic Party.

September 2015 – Muslim separatist leaders in Kashmir closed shops, businesses and government departments in protest at the enforcement of a ban on eating beef.

July 2016 – The killing of Burhan Wani, a popular militant and top commander of the Hizbul Mujahideen group by the security forces sparked violent protests. Subsequently, a curfew was imposed in most parts of Kashmir.

August 2016– Curfew lifted from most parts of Kashmir. At least 68 civilians and two security officials died and more than 9,000 people were injured in over 50 days of violence according to official tallies.

Kashmir: Indian and Pakistani narratives:

The Indian view:

- Maharaja Hari Singh signed the Instrument of Accession in October 1947, handing control of the Kingdom of Jammu and Kashmir over to India.
- Also, the UN Resolution in 1948 accepted India's stand regarding all outstanding issues between India and Pakistan.
- Pakistan has not removed its military forces from the region, which India views as one of the first steps in implementing a resolution.
- India accuses Pakistan of funding military groups in the region to create instability, and accuses Pakistan of waging a proxy war.

- According to India, most regions of PoK, especially northern areas, continue to suffer from lack of political recognition, economic development and basic fundamental rights.

The Pakistani view:

- Pakistan claims that according to the two-nation theory Kashmir should have been with Pakistan, because it has a Muslim majority.
- Pakistan argues that India has shown disregard to the resolutions of the UN Security Council, and the United Nations Commission in India and Pakistan, by failing to hold a plebiscite.
- Pakistan rejects Indian claims to Kashmir, centering around the Instrument of Accession. Pakistan insists that the Maharaja did not have the support of most Kashmiris. Pakistan also claims that the Maharaja handed over control of Jammu and Kashmir under duress, thus invalidating the legitimacy of the claims.
- Pakistan claims that India violated the Standstill Agreement and that Indian troops were already in Kashmir before the Instrument of Accession was signed.

Root causes behind the Kashmir unrest

1. A confrontation between two nationalisms:

- For **India**, the question of Kashmir, is not merely one of retaining a small part of its territory; it impinges on the very basic character of the Indian state and society. If Kashmir seceded from India on grounds of religion, the two-nation theory would seem to have been vindicated. It would strengthen the Hindu communal forces and pose a serious threat to millions of Muslims, whose number in India is larger than even that in Pakistan, making their position in India quite untenable.

- Since Kashmir is predominantly Muslim, **Pakistan** believes it should belong to them. Moreover, Kashmir has to be won to justify the religious moral significance of Pakistan's nationhood.

2. Political causes

India and Pakistan both believe that they have a rightful claim to Kashmir. (See the previous section)

3. Economic Causes

- Even while militancy was in decline and a free and fair electoral system in place since 2002, the governance deficit remained large. Economic growth in the state almost consistently lagged behind the national growth figures.
- Widespread unemployment and lack of new job avenues
- Disintegration of traditional handicrafts
- Poor industrial setup
- Declining tourism due to terror attacks
- Loss of crops due to floods, cloudburst etc.
- Issues in rehabilitation of flood victims etc

4. Social causes: Poor education and health system, allegations of penetration of radical Islam in the majorly Sufi Islam region, wounds of 1980's insurgency and indoctrination of youth by radical leaders has further contributed to their despair.

5. General disenchantment with constitutional measures

A general absence of good and sound administration with allegations of corruption and nepotism coupled with allegations of electoral frauds in the initial years lead to a loss of faith in the legitimacy of the constitutional measures.

Laws like AFSPA, regular curfews, presence of armed forces, allegations of human right violations etc have contributed in increasing anger of the people against the state.

6. A large role for the army in Kashmir has been a necessity in view of Pakistani military threat and subversion; but this has also meant a high cost in terms of the functioning of a civil libertarian polity.

7. A demand for greater political autonomy for the region

8. An atmosphere of mistrust:

Fear and mistrust are central to this conflict. Fear of people belonging to another religion having a different value system that threatens one's own, as well as fear concerning the loss of control or the loss of power. This fear has paralyzed progress towards peace as it works against the one ingredient which is essential for positive change: trust.

9. Stereotyping

Elites from both India and Pakistan stereotype the opposite country. This is the result of misappropriation of information in the **education system** as well as in the **media**. History textbooks, for example, distort history to reinforce a particular image, providing an enduring basis for hatred; children are thus socialized at a young age by what are often blatant factual errors. Similarly, mass media present few programs that humanize the other by reflecting true realities and similarities, focusing instead on stark differences and problems.

10. External factors:

- Pakistan incites the sentiments of Kashmiri people especially youth, carries on cross-border infiltration to spread the unrest and uses terrorism as a diplomatic tool to worsen the situation.
- Chinese support to Pakistan in an attempt to balance against India.
- Islamist fighters from various countries have declared the conflict a Muslim cause.

Factors which have fuelled unrest in the region in recent times:

- Use of **social media** for false rumours to instigate youth to lead violent mobs

- Stone pelting on security forces by radicalised and incited **youth**
- Armed militants mixing with stone-pelting mobs and addressing rallies
- Militants using cover of "agitating mobs" firing at security forces and lobbing grenades, **provoking security forces** to retaliate
- Attacks/threats on government officers, political representatives and policemen
- **No identifiable leadership** of protests
- The challenge of **radicalization** of youth.

5.COMMUNAL VIOLENCE

Introduction

Communalism, is referred in the western world as a "theory or system of government in which virtually autonomous local communities are loosely in federation". Communalism is a political philosophy, which proposes that market and money be abolished and that land and enterprises to be placed in the custody of community. But in the Indian sub-continent context, communalism has come to be associated with tensions and clashes between different religious communities in various regions.

Development of communalism as political philosophy, has roots in the ethnic and cultural diversity of Africa. It is characterized as, People from different ethnic groups or community, who do not interact much or at all and this has somewhere acted as hindrance in the economic growth and prosperity of Africa.

Communalism in South Asia is used to denote the differences between the various religious groups and difference among the people of different community. And generally it is used to catalyse communal violence between those groups.

Communalism is not unique only to South Asia, but is also found in Africa, America, Europe, Australia, and Asia. But, it is significant socio-economic and political issue in Bangladesh, India, Pakistan, Myanmar, Sri Lanka, Nepal, etc.

What is Communalism?

It is basically an ideology which consists of three elements:-

- A belief that people who follow the same religion have common secular interests i.e. they have same political, economic and social interests. So, here socio- political communalities arises.
- A notion that, in a multi-religious society like India, these common secular interests of one religion are dissimilar and divergent from the interests of the follower of another religion.

- The interests of the follower of the different religion or of different 'communities' are seen to be completely incompatible, antagonist and hostile.

Communalism is political trade in religion. It is an ideology on which communal politics is based. And communal violence are conjectural consequences of communal ideology.

Evolution of communalism in Indian society

If we discuss about Indian society, we will find that, ancient India was united and no such communal feelings were there. People lived peacefully together, there was acceptance for each other's culture and tradition. For example, Ashoka followed religious tolerance and focussed mainly on Dhamma.

In Medieval period, we have examples such as- Akbar, who was epitome of secular practises and believed in propagating such values by abolishing Jajhiya tax and starting of Din-I- ilahi and Ibadat Khana. Same acceptance for different cultures and tradition was practised in several kingdoms throughout India, because of which there was peace and harmony, barring few sectarian rulers like Aurangzeb, who was least tolerant for other religious practises. But, such motives were guided purely for their personal greed of power and wealth.

Such rulers and actions by them like- imposing taxes on religious practises of other community, destructing temples, forced conversions, killing of Sikh guru, etc. were instrumental in deepening and establishing the feeling of communal differences in India. But, these incidents were not common as, huge majority of Indians were rural and were aloof from such influences and so people coexisted peacefully. Though, they were very rigid in practising their own rituals and practise, but it never became barrier in the peaceful coexistence. Overall, the Hindus and Muslims in those days, had common economic and political interests.

Communalism in India is result of the emergence of modern politics, which has its roots in **partition of Bengal in 1905** and feature of separate electorate under **Government of India Act, 1909**.Later, British government also appeased various communities through **Communal award in 1932**, which faced strong resistance from Gandhi ji and others. All these acts were done by the British government to appease Muslims and other communities, for their own political needs. This feeling of communalism has deepened since then, fragmenting the Indian society and being a cause of unrest.

(by Communal award colonial government mandated that consensus over any issue among different communities (i.e. Hindu, Muslims, Sikhs and others) is precondition for any further political development)

Communal consciousness arose as a result of the transformation of Indian society under the impact of colonialism and the need to struggle against it.

Stages in Indian Communalism and how it spread

India is a land of diversity. And it is known for lingual, ethnic, cultural and racial diversity. As, we have discussed above, communalism in India is a modern phenomenon, which has become threat to India's *Unity in Diversity*. We will see the various stages:-

- First stage was **rise of nationalist** Hindu, Muslim, Sikh, etc. with only first element of communalism as discussed above. Roots of this were led in later part of 19th century with Hindu revivalist movement like *Shuddhi movement* of Arya Samaj and Cow protection riots of 1892.

  On the other hand movements like Faraizi movement started Haji Shariatullah in Bengal to bring the Bengali Muslims back on the true path of Islam, was one of the religious reform movement which had bearing on communalism in 19th century. Later people like Syed Ahmed Khan, who despite of having scientific and rational approach, projected Indian Muslims as a separate community (qaum) having interest different from others.

- Second stage was of **Liberal communalism,** it believed in communal politics but liberal in democratic, humanist and nationalist values. It was basically before 1937. For example organisations like Hindu Mahasabha, Muslim League and personalities like M.A. Jinnah, M M Malviya, Lala Lajpat Rai after 1920s
- Third was the stage of **Extreme Communalism,** this had a fascist syndrome. It demanded for separate nation, based on fear and hatred. There was tendency to use violence of language, deed and behaviour. For example Muslim League and Hindu Mahasabha after 1937.

It *spread* as a by-product of colonialism, economic stagnations and absence of modern institutions of education and health. These factors caused competition, people started using nepotism (patronage bestowed or favouritism shown on the basis of family relationship, as in business and politics), paying bribes to get job,

etc. Short term benefits from communalism started giving validity to communal politics.

Later on, spread of education to peasant and small landlords gave rise to new middle class, as agriculture was becoming stagnant. So, these people started demanding communal representation and this way, social base for communalism widened. Middle class oscillated between anti-imperialism and communalism. Communalism, started rooting deeply, as it was an expression of aspiration and interest of middle class for less opportunity.

Further, from very beginning upper caste Hindus dominated colonial services as they adapted early to colonial structure. Because of Mughal rule and 1857 revolt, colonial government was suspicious towards Muslims and they patronised Hindus. This resulted in resentment in Muslims in late 19th century and they then formed a pressure group under Sir Sayed Ahmed Kahn to bargain as a separate community. In contrast Congress standpoint was always focused on 'rights and freedom of individual' not on a particular community

In several part religious distinction coincided with social and class distinction, causing communal distortion. Communal outlook was given, not by participants but by the officials, politician and journalists. In fact agrarian conflicts, did not assume communal colour until 20th century. For example- Pabna agrarian movement.

Communalism represented a struggle between two upper classes / strata for power, privileges and economic gain. For Example- In western Punjab at that time, Muslim landlord opposed Hindu moneylenders. In eastern Bengal, Muslim *jotedars* opposed Hindu *zamindars*. Later on, communalism developed as weapon of economically and politically reactionary social classes and political forces.

Divide and Rule

Communalism was a channel for providing service to colonialism and the jagirdari class (land officials). British authorities supported communal feelings and divided Indian society for their authoritative ruling. As we have already discussed above about separate electorate, like that official patronage and favour having communal biasness was very common. Communal press & persons and agitations were shown extraordinary tolerance. Communal demands were accepted, thus politically strengthening communal organizations. British started accepting communal organisations and leaders as the real spokesperson of communities and adopted a policy of non-action against communalism. In fact, for the same reasons even the communal riots were not crushed. Separate electorate started in 1909 to communal award in 1932 fulfilled the wishes of British authorities of ruling India by dividing the societies on communal lines.

In parallel there was introduction of strong Hindu religious element in nationalist thoughts and propagandas. For example Bal GangadharTilak popularised Ganesh pooja and Shivaji Mahaotsav and taking dip in Ganga,etc. The programmes related to "Ganesh Pooja" and "Shivaji Mahotsav" was not initiated to support the interests of Hindus. However, both "Ganesh" and "Shivaji" were associated with the emotions of a number of Hindus. This was to be used by Leaders as tool to politically awaken Indians. But, Indian history in schools and colleges were given Communal and unscientific colour. This kept Muslims largely away from Congress till 1919. In early decades only 8-9% of members of Congress were Muslims.

Gradually religiosity became major contributory factor and it started intruding the non-religious and non-spiritual areas of life and also beyond the individual's private life.

Though, India is a secular country but due to communal feelings the secularization is getting affected. Secularization is narrowing down the sphere of religion to the private life of the individual. So, communalism is basically becoming a belief system through which a society, economy, and polity are viewed & expanded and around which effort is being made to organise politics.

With these unprecedented changes, the best atmosphere of communal harmony should have been created in India and according to the expectation of Mahatma Gandhi this country should have become an example in this direction. But this did not happen.

Why communalism still persists and increasing in modern India?

Constitution of India, gives certain fundamental rights to the citizens (i.e. individuals). But in case of minorities, the whole community has been given fundamental rights under Article 28,29 and 30, according to which they are free to manage their educational institutions and have right to conserve their own culture. But these rights are being used, above the individual rights by the personal law boards guided by their own community laws. As it was seen in *Shah Bano case.*

There is also resentment against such personal laws and clamour is increasing for **Uniform civil code**, which is also mentioned under Article 44 in Directive principle for states of Indian constitution. This will help in narrowing the religious cleavages.

In absence of Uniform civil code, there is still perception that all communities have divergent and contradictory interests. Consequently, community based pressure groups bargain for their own community. At political level these communities compete for power and resources. This competition, in turn, escalates to major conflicts. Politicians try to turn these communities into vote banks and different communities become watertight compartments.

Since Independence, India has been pursuing the ideal of nation-building based on secularism. Even after 68 years of independence, India is still burning under the fire of communalism. Though, there are various reasons responsible for this. But few of them have been discussed here, understanding the reasons which play role in continuation of communalism are:-first one is religious, and the second one is political. Third one is socio-economic and the fourth one is international.

In the first, i.e. religious, its fundamentalism should be considered responsible for communalism. After all, **'Our belief alone is true'** and **'rest is untrue or incomplete',** we find this kind of mentality of fundamentalists. As per this mentality, when the followers of any religious community, sect or sub-sect indulge in their activities, they certainly come in conflict with others. Reason is quite evident. They do not have tolerance, which is absolutely necessary for a country like India–a land of different religious communities. They become the cause of confrontation, malice and struggle.

Politicians also have played a villainous role in creating serious communal situations in India. There was politics at the root of painful division of India in 1947 in the

name of a particular religious community. But even after paying a heavy price in the form of partition, in many riots provoked thereafter, we can find the involvement directly or indirectly, of political parties or their supporters. Along with this for the sake of vote bank, the policy of appeasement, selection of candidates on the basis of community, sect, sub-sect and caste, and flaring up religious sentiments at the time of elections, led to the rise of communalism. These practices are still continued and the country is bearing heavy loss because of it. We can witness many adverse results of these practices.

Socio economic conditions of India, though after independence has improved and even the economic reforms after 1991 has been instrumental in improving such conditions, but still there are many challenges in front of Indian society, which are becoming threat for its diversity. Population, Poverty, illiteracy and unemployment create a lot of compulsions, especially before younger generation. That is why, many from younger generation, because of lack of right thinking, remain unemployed and in a state of poverty, get involved in the evil like communalism. The efforts being made for uprooting poverty, illiteracy and unemployment are not as fruitful as they should be.

External elements (including non-state actors) also have a role in worsening the problem of communalism, and making it serious. We cannot mention the name of any particular country in this regard but scholars and those who think on this problem from time to time have highlighted this fact.

The main reasons for involvement of external elements or their role in riots are as follows:

- To create an atmosphere of instability, so that it becomes socially weak;
- To hope for gaining sympathy from minorities;
- To try to weaken the economic structure of a foreign country; and
- With the aim to conceal their own incompetence.

Infamous communal violence in India

- **Partition of India,1947**

  After partition, millions of population were forced to move from both sides of the border. Hindus in Pakistan and Muslims in India were killed in masses, women were raped, and many children lost their parents. There was hatred everywhere, violence didn't see anything except bloodshed. Later, it turned in the problem of refugees and their rehabilitation became one of the biggest challenge for independent India.

- **Anti-Sikh riots, 1984**

  This is one of the bloodshed in India, where Sikhs in large number were massacred by anti- Sikh mob. This massacre took place in response to the assassination of Prime Minister Indira Gandhi by his own Sikh body Guard in response to her actions authorising the military operation.

- **Ethnic cleansing of Kashmiri Hindu Pundits in 1989**

  Kashmir is known as the heaven of India and was known for its *Kashmiryat,* i.e. the reflection of love, peace and harmony through brotherhood and unity of Hindu, Muslims and other communities living together. But, the brotherhood saw a serious blow due to Extremist Islamic terrorism in the Kashmir valley, which led to mass killing and large scale exodus of Kashmiri Pundits from the valley to the various regions and corners of the India, giving them the status of refugee in their own country. Since then, the valley is under the grip of communal violence and the ongoing unrest has become a problem for the development of the people.

- **Babri masjid demolition in Ayodhya, 1992**

  According to Hindu mythology, Ayodhaya is birth place of Lord Rama and therefore it is sacred place for Hindu religion. But in medieval period Mughal general Mir Baqi, built a mosque, named after Mughal ruler Babur. There were disputes since then and riots also took place. But in 1990, due to some political mobilisation, there was atmosphere of protest by Hindu religious groups and in large scale "kar sevak" visited Ayodhya from all parts of India, in support of demolishing Babri masjid and building Ram temple there. These movements caused huge amount of bloodshed and since then it is a disputed matter.

  After this, violence was followed by the Godhra incident in 2002, when "kar sevak" returning from Ayodhya in a Sabarmati Express were killed by fire in the coaches of train. This act was followed by the extended communal violence in Gujarat. That violence is like black spot in the history of the Gujarat and nation too, as people were killed without any mercy. Hindu and Muslim community became antagonist to each other. Till now people are fighting for justice in Supreme Court, with a ray hope from the Indian Judiciary.

- **Assam Communal violence,2012**

  North eastern states are known for its distinguished tribal population & ethnic diversity and large scale Bangladeshi immigration has changed the demography of North eastern states, which often becomes reason for clashes. In 2012, there were ethnic clashes between Bodos (Tribal, Christian & Hindu faith) and Muslims. Ethnic tensions between Bodos and Bengali-speaking

Muslims escalated into a riot in Kokrajhar in July 2012, when unidentified miscreants killed four Bodo youths at Joypur.

- **Muzaffarnagar violence, 2013**

  The cause of this ethnic clash between Jat and Muslim community is very much disputed and has many versions. According to few, it was started after some suspicious post on Social media platform Facebook. According to some, it was escalated after the eve teasing case in Shamli. Let the reasons be unknown, but what matters is, the nature and scale of loss to the country with respect to human resource and peace.

In all these and hundreds of other riots, one thing is common that huge majority of victims have nothing to do with communal hatred. In short, preparators of violence and victims of violence are different persons.

Similar to above mentioned list, there are many more, which has impact on the masses and killed people on large scale. Bombay bomb incident, 1993, Attack on Akshardham in 2002 by Lashkar-e-Toiba & Varanasi Bomb attack, 2006 are few of them, having Anti-Hindu outlook.

Lot of movies have been pictured on the above mentioned communal violence, which can give us understanding about the damages and harm, done by these violence- **"Bombay"** & **"Black Friday"** based on 1992 attacks. **"Train to Pakistan"** based on the novel of Khuswant singh about partition of India, 1947. **"Gandhi"** is portrayal of Direct Action Day and partition of India. "**Hawayein**" based of 1984 Sikh riots and "**Machis**" about Punjab terrorism.

Consequences of communalism

Consequences of communalism is well known to all of us. With killings in mass, the real sufferers are the poor, they lose their house, their near and dear ones, their lives, their livelihood, etc. It violates the human rights from all direction. Sometimes children will lose their parents and will become orphan for life time and nobody will be there to look after them.

Ghettoization and refugee problem is the other dimension of communalism induced violence, whether its inter country or intra country. Sudden increase in violence against any particular community causes mass exodus and stampede which in turn kills many number of people. For example, this was seen in the case of Bangalore in

2012, with respect to people from North eastern states, which was stimulated by a rumour.

Apart from having effect on the society, it is also a threat to Indian constitutional values, which promotes Secularism and religious tolerance. In that case, citizens don't fulfil their fundamental duties towards the nation. It becomes a threat for the unity and integrity of the nation as a whole. It promotes only the feeling of hatred in all directions, dividing the society on communal lines.

Other than these, minorities are viewed with suspicion by all, including state authorities like police, para military forces, army, intelligence agencies, etc. There have been many instances when people from such community have been harassed and detained and finally have been released by court orders guilt free. For this, there is no provision of compensation of such victims, about their livelihood incomes forgone, against social stigmas and emotional trauma of the families.

Such things are set back for the society and becomes barrier for its development. This is also one of the reason which is keeping India still under the status of "developing nation" because, such activities occurring frequently do harm the human resource and economy of the country. And then again it takes years for the people and the affected regions to come out the traumas of such violence, having deep impact on minds of those who have faced it. Whole life, they feel emotionally broken and insecure. How can we imagine in such conditions, for timely harvest of demographic dividend?

Government iniatives

National human rights commission (NHRC) in India fights for the causes of rights of the victims, but its recommendations are advisory in nature, which doesn't gives significant outcome.

From time to time, respective governments have constituted various committees, to give recommendations to solve the issue of communal violence. Prominent among them are SACHAR COMMITTEE, NANAVATI COMMITTEE and RANGANATH MISHRA COMMISSION.

The **Nanavati-Mehta commission,** set up by Gujarat government in 2002 to enquire about Gujarat violence.

Sachar committee, appointed in 2005, recommended to set up **Equal opportunity commission (EOC)** in 2010. EOC was to set up a grievance redressal mechanism for all individual cases of discriminations- religion, caste, gender & physical ability among others.

The **Ranganath Misra Commission** was entrusted by the Government of India to suggest practical measures for the upliftment of the socially and economically backward sections among religious and linguistic minorities and to include the modalities of implementation for the same. The report of the National Commission for Religious and Linguistic Minorities, headed by former Chief Justice of India Rangnath Mishra, says that 10% should be reserved for Muslims and five% for other minorities in central and state government jobs in all cadre and grades.

The purpose of all above committees is to give recommendations to find out the causes of backwardness of minorities and steps required to improve their conditions.

Ranganath Misra Commission

The Indian law defines communal violence as, "any act or series of acts, whether spontaneous or planned, resulting in injury or harm to the person and or property, knowingly directed against any person by virtue of his or her membership of any religious or linguistic minority, in any State in the Union of India, or Scheduled Castes and Scheduled Tribes within the meaning of clauses (24) and (25) of Article 366 of the Constitution of India"

Though India is under the grip of communal violence, but till now, other than provisions under **IPC and CrPC**, there is no firm law to punish the originators of such violence, no clear policy for relief and rehabilitation of victims. There is no regulations for security of witness, for accountability of public servants, etc.

'Prevention of Communal and Targeted Violence (Access to Justice and Reparations) Bill, 2011' lapsed in the parliament. The bill provided for a seven-

member *National authority for communal harmony, justice and reparations*. It attempted to safeguard the minority sections. It had provisions for ensuring accountability of the district administration. This has already been recommended by the Sachar committee and Raganath Mishra Commission.

The role of police in communal riots is highly controversial. Generally, riot victims complain that- police did not came to rescue, police forces were themselves instrumental in the killing, they led the mob in looting and burning, arrested the innocent people and harassed them inside the lockup, etc. But as we know, that police can act much better, if there is political will and if they are given free hand along with the implementation of recommended police reforms.

There specialised battalions of **Rapid Action force** in India, which is a wing of CRPF, to deal with riots, riot like situations, crowd control, rescue and relief operations, and related unrest

Steps required

The solution of such problems cannot be one or two steps by government. Apart from legislative support, administrative efficiency and alertness with the help of modern tools and technology, the major onus lies on the citizens themselves by avoiding communal violence. Though its bit philosophical in nature, as it's not a concrete solution, but the sustainable changes can be brought only by those steps.

Each of us, have to make a balance between our own religious community and national interests, we have to unite with nationalism, and then should move forward. The teachings of a religious community may be great, but the followers of the community concerned should understand that nationalism is greater. If they do not become familiar with this fact, they will be away from national stream; they will suffer. This fact relates not only to India but also to many other countries of the world.

We have to be rational while making decisions. Each and every religious community has been founded on the basis of certain values that were best and necessary for circumstances of the country and times. Goodness like adjustment with others, or co-operation, or consistency can be found in their teachings. But by not moving according to the teachings of their religious community those who depend upon fundamentalism and conservative practices, or those who use their co-religionists taking advantage of their poverty, illiteracy or innocence, are dishonest towards their own self, their co-religionists and also towards those great leaders who founded the religious community. Everyone must understand this fact also. Along

with this, leaders of all communities, by knowing it, must come forward for an atmosphere surcharged with harmony, in which lies their welfare too. The religious teachers should promote rational and practical things through religion promoting peace and security.

Policies like appeasement, fun and frolic with the sentiments of people for individual and party interests, and selection of candidates on the basis of religious community or sect by keeping aside the qualifications, one, certainly, does the things against national interest or nationalism; are reflections of lower national thinking. That is why; these kinds of acts should be stopped at government level and also at the level of political parties.

There is a great need to work towards eradicating the problem of unemployment among the youths, illiteracy and poverty and that too with honesty and without any discrimination. This will help in solving many problems, and will create awakening. The result will be in checking on communalism to a great extent. That is why it is expected that a lot of work have to be done at government level in this direction.

But whatever have been mentioned in above paragraphs, will be effective only when our society and its citizens, become so much capable and empowered, that they can take sensible, ethical and rational decisions. This is possible only with the help of quality education. But quality education for such huge population, cannot be always expected from the public institutions. It is also the corporate social responsibility, it is the responsibility of the educated Indians, NRI and everyone who has roots in India to bring changes in Indian society. So that we can live, the ethos of our constitution and would be able to promote International peace and security too.

Media, movies and other cultural platforms can be influential in promoting peace and harmony. Though all such practises in India are common, but there is still scope for improvement in this direction.

Thus, in order to get rid of the problem of communalism in India, there is a need of collective efforts. All will have to discharge their duties. If we do so, definitely harmony will prevail. Everybody will prosper. This must be done; this was the dream of Mahatma Gandhi for a free India.

Challenge of social media and Freedom of expression

Now a day's social media has become notorious for spread of communal hatred. It provides almost instant transfer of provoking material on which our government has

no control. It has become potent tool in hands of religious bigots to spread hatred for other religions.

It is true that, Fundamental Rights, under article 19(1), gives citizens freedom of expression. But proviso to this article also empowers government to impose reasonable restrictions to guard unity and integrity of the country. Further, under Fundamental Duties 51A constitution provides –

"(e) to promote harmony and the spirit of common brotherhood amongst all the people of India transcending religious, linguistic and regional or sectional diversities; to renounce practices derogatory to the dignity of women"

This needs to be enforced by state by controlling social media. In olden days, whenever any provocative print media came government invoked its powers and imposed restriction, but yet government has no strong/effective policy towards social media.

Conclusion

Communal violence is common now days throughout the world. They are known by various alternative names, as in China, the communal violence in Xinjiang province is called ethnic violence. Communal violence and riots have also been called non-State conflict, violent civil or minorities unrest, mass racial violence, social or inter-communal violence
and ethno-religious violence.

Violence between Buddhists and the Muslim Rohingya, inhabit Rakhine state (formerly Arakan province) which stretches along most of Myanmar's coast up to the Bay of Bengal and borders the Chittagong province of Bangladesh, erupted in 2013. Such violence in neighbouring countries like Myanmar, Bangladesh, and Pakistan causes violence in retaliation in India also. It also catalyses the problem of refuges, as in case of Pakistani Hindus, etc. Sri Lanka is also facing international critics and United Nations related to ethnic clashes and action of government against minority Tamilians, which has direct bearing on India and Sri Lanka relations and India's internal security.

Increasing diversity, due to influx of populations from all corners of world in western countries like USA, UK, Canada, Australia, etc. is posing the challenge of ethnic clashes and violence in their respective societies.

Communalism can be combated with the help of globalisation as a tool. In the globalised world, all countries are becoming integrated and dependent on each other. Movement of people from one place to other is becoming very easy, in such conditions to avoid such potential violence, governments are already promoting cultural exchanges through shows, programs, heritage walk, cultural visit by students and parliamentarians. Promoting learning of each other's local language for easy exchange of ideas. With respect to this, recently US President Barak Obama's message on Diwali festival can be seen as an active step to promote cultural mingling and living peacefully. If all the countries cooperate with each other, they can face and solve even the deadliest challenge of terrorism and groups like Al-qaeda, ISIS,etc.

6. LINKAGES BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM

In Indian scenario, extremism activities are increasing rapidly. The scale of the extremists operations is massive and consequently these activities have perilous impact on nation's social, economic and political development.

Many scholars explained the notion of extremism as any ideology considered to be far outside the normal attitudes of society or to interrupt common moral standards. It is usually constructed with moderation or extremists with moderates. Various political writers signified that extremism also has numerous strands starting from just holding to one's ideas and values on one end of the continuum and use of violent means for nuisance on the other end. Thus, extremism is considered as a complex phenomenon.

Causes of extremism: There are numerous of reasons for the development of Extremism in India:

1. Lack of governance: Governance is mainly concerned the significant issue as that lack a long term strategic perspective. Priority of Government bodies is to focus on Industrialization and do not give much importance to people living in tribal areas. Tribal have been denied their constitutional rights and justice.

2. Socio-economic issues: When considering socio economic issues, education must be the prime involvement and this needs to be addressed with innovation. Once populace is literate and well educated in particular region, they will be able think logically and do not involve violent actions. Most of these people who are entering into the movement of extremism are lacking primary education, basic amenities and infrastructure facilities.

Economic discontent was a prevailing factor which led to the growth of the militant nationalism. Towards the end of the 19th century economic condition of the people became miserable due to unemployment and repressive financial measures of the Government.

In all over worlds, following causes can be observed for growth of extremism:

1. Political deprivation leading to hopelessness or a sense of powerlessness.

2. Long festering political disputes.
3. Lack of Education and poverty.
4. Ideological imperatives may lead to extremism.
5. Socio-economic inequities, unemployment, despair about the future.
6. Dishonest and self-serving dominant groups.
7. Foreign occupations.
8. Sense of victimhood amongst Muslims.
9. Renaissance of Islam phobia in Europe.

Types of Extremism:

1. Personal Extremism
2. Family Extremism
3. Institutional or Organizational Extremism
4. Group Extremism
5. Social or Cultural Extremism
6. National Extremism
7. International Extremism

Determinants of Extremism:

Extremism is just like epidemic ailment that spread its arms in various parts of world. There are three important determinants. First the extremism that those in power exhibit. They go in with tanks and bombs where persistent force backed diplomacy can work, seek to destroy what requires careful reconstruction, advance division and hate where understanding and bridging of differences is needed, and abandon the path of justice and fair play for pure partisanship. All this naturally promotes lethal and devastating extremism. Secondly, when political system is not credible and there is no reliable justice structure, political groups often frame their concerns and solutions in an extremist way. When a non-credible political system leads to the illegal imposition of the rule of a specific elite, party, ethnicity or institution over the 'rest', the response of the rest is often cast in extreme ethnic, religious, anti-elite or anti-institution character. Henceforth through overemphasis of their legitimate concerns, they construct a victimhood scenario. In countries where trustworthy political and legal systems do not exist, many would buy into victimhood framing. The causes of dissatisfaction may be plentiful. They could be political, cultural, sociological, economic and moral. Third determinant of extremism is perpetual discontent that develops frustration, irrationality and worry and a mind that will almost naturally take to radicalism. They have almost no stake in the dominant socio-political and cultural milieu. With lots of suffering, people

choose path of the anarchistic, nihilistic or messianic route to worldly and heavenly deliverance.

Developmental issues associated with development and spread of extremism:
Natural Calamities: During the last decade of the 19th century, affliction of people was filled to the brim. Famine, plague, earthquake, war and repressions were let loose in the country. From 1896 to 1900 prolonged and catastrophic famines occurred throughout the length and breadth of the land in a bewildering succession. In 1896 bubonic plague broke out in Bombay and took a toll of millions of lives. These natural calamities were accompanied by the intensified exploitation and suppression by the Government. Such devastating conditions led to development of extremist.

Special Economic Zones:
Spread of extremism is a major issue for any country. Land acquisition for Special Economic Zones created chaos among tribal people and they come to street for protest. Large tracts of land are being acquired across the country. There is a loss of revenue in the form of taxes and it greatly impacts on agricultural production. Land is living resource for farmers and their life is dependent up on the land. Special Economic Zones needs a single huge block of land and government is now taking stern steps to acquire the land. Mediators are also generating trouble between government and farmers. Such situation is very disturbing for farmers and they lose huge money. Government compensation is also not justified as it is very low. Such factors enforce people to become violent and give rise to their extremist activities.

Labour, Unemployment and wages:
Another intense issue that spreads extremism is joblessness which creates insecurity of living. People may develop dissatisfaction and anger both in urban and rural areas. In allocation of government jobs, there has been shown some favouritism and this activity leads to dissatisfaction among youth as they are being ignored.

Policing:
Improper policies and their ineffective implementation may result in extremist activities among weaker sections of society. It is very necessary that government must consider poor people when devising policies for economic growth of country. These policies must be well-organized and unprejudiced which reveal good administration .Weaker section of people does not have much confidence in police. People have no faith that justice will be done to them against the powerful person in

the society. Such impression about government officials develops extremist thoughts among poorer section of society.

Process of getting Justice:
When lower section of society is struggling with various issues related to survival or employment and their conflicts and disputes are not settled in time, frustration among people in society develops. Presently, judicial system of India is very time consuming and disputes are not settled in short time. The parties to the dispute lose control over even the terms and details of the dispute once it goes to the court. These factors create extremist feelings among sufferers.

Ways to resolve issue of extremism:
Land Related Measures:
It is necessary to make efforts to continuously implement the land ceiling issues. So that the ceiling excess land obtained should be made available for distribution amongst the most susceptible section of the landless poor people. Land should be acquired by government for special economic zone through giving proper compensation to the agriculturalists.

Basic facilities and Infrastructure:
It is observed that when government fails to provide infrastructure and services as per national norms that gives rise extremism affected areas. Basic services to standards among the people in these areas are to be given prime importance.

Governance Issues:
There are some government issues that lead to spread of extremism. In central India where disturbance is prevalent such as states like Andhra Pradesh, Orissa, Chattisgarh, Madhya Pradesh, Jharkhand and parts of Maharashtra. State interventions both for development and for law and order are not good. Local populations present in the tribal areas are being dominated by the armed and rich people. Government must take necessary steps to protect these communities. The basic steps to improve the status of poorest section of society is establishment of credibility and confidence of government, keeping a continuous watch for fulfilment of peoples vision, effective protection, peace and good governance, sustainable development with equity in tribal areas, will make extremism low in tribal areas.

Government initiative to decrease extremism:
Government must come forward to reduce the expansion of extremism in India through implementing various policies. Military operations have not been

uncontrolled and individual states continue to undertake area clearing operations, such exercises appear to form parts of a new clear, hold and develop strategy that uses development as a tool to win back the support of the tribal population, who overpoweringly appear to sympathize with the extremists. In the beginning of 2011, there is a rehabilitated focus to perform development initiatives in areas cleared of Maoist presence. Several flagship projects of the government to improve connectivity of tribal areas with the administrative centres, to provide work to the tribal youth and to make certain health and educational facilities have been launched. It is imperative to ensure that proper execution of these developmental projects and monitor their progress, a new scheme titled Prime Ministers Rural Development Fellows Scheme has also been revealed. Under the scheme, 156 young professionals have been trained and are being stationed in 78 worst-affected districts for two years to help the district administration. Resources have started flowing into the coffers of the district administration with an importance on time bound utilization and execution.

It has been observed in the past that the extremists targeted infrastructure projects or have prevented contractors from completing the projects, security forces are now allocated to protect the planned development ventures in order to ensure their timely completion and security. Government must assure to people of weaker section that they will not harm the tribal community.

The government has also cleared a proposal to raise a combat unit under the para-military Central Reserve Police Force (CRPF) for construction of roads in Maoist-affected areas.

India is currently dealing with an effective response to left-wing extremism. Even though in the last two years, extremist ferocity as well as areas under extremist influence has somewhat reduced, but the problem remains.

To summarize, extremism is entrenched in Indian community. Various authors elaborated this concept as violent activities of certain group of people due to dissatisfaction from government policies and initiatives. It is established that Extremism became a major philosophy of Indian nationalism. There are several grounds for development of extremism in India such as joblessness, ignorance of weaker section of society by government. After thorough review of causes and issues for the development of extremism, it is revealed that extremism is viewed differently by dissimilar sections of the society. On one side, there are passionate supporters and, at the other extreme, some others hold the view that the movement should be crushed cruelly. It is difficult to classify the opinion in the middle path. It can be said

that some of the demands of the extremists are genuine and cannot be ignored. Therefore, the Government must seriously consider such demands and make policies and execute them, either voluntarily or subsequent to negotiations with the protestors.

Evolution of Indian Left wing

Communist Party of India (CPI) was formed in 1920's under the aegis of MN Roy in Tashkent. At the same time there was wave of Socialism blowing in India motivated from Russian revolution and vagaries of Economic Depression. Colonial government was quite nervous and it frequently cracked any plans of socialist minded people conspiring against it. 1st such crackdown was Peshawar Conspiracy Case, then came Kanpur conspiracy case in 1924, and later Meerut Conspiracy Case in 1929. With all this, people only got more attracted to and aware of socialist ideas. Meanwhile, numerous small and regional organizations came under mainstream Communist Party of India in 1925.

After, 1929 broke away from mainstream politics which was led by congress and took its own course. This was due to decision taken at Congress of Communist International, which branded congress as party of Bourgeoisie, which is colluding with imperialists to further its own ends. Later they opposed Quit India Movement because Britain was with Russia against Germany in World War.

Extremist Left wing movement was present at time of Independence mainly in Hyderabad and Patiala princely state. Communists affiliated by CPI, here came to rescue oppressed peasants from Jagirdars and biswedars. In Hyderabad they fought against Islamic militia, the Razakars. When Indian army liberated Hyderabad in 1948, communists who were deeply influenced by Russian Revolution, decided to continue their struggle against bourgeois Indian government. They were soon pursued by Indian forces and by 1951, movement's back was broken. Similarly in Punjab, a small band of militia was formed to protect farmer from oppressive biswedars and soon it got eradicated.

After brutal repression by state CPI gave up armed struggle and joined democratic politics. In 1957, it emerged largest opposition party and in same year it came to power in Kerala and EMS Namboodiripad became chief minister. It was 1st democratic government under a communist party all over world.

In 1962 when Indo-China war broke out majority of CPI leaders viewed it as struggle of a socialist country against Capitalist India. Consequently, they supported China's cause, due to which Govt. put many leaders in jail. Further, there was growing

dissent in party for party's diversion toward democratic state which was contrary to Communist principle of armed struggle to overthrow the state. It was felt by some leaders that they are getting absorbed into present system. This finally culminated into split in the party in 1964 which resulted in new party called Communist Party of India (Marxist).

Dissent and differences didn't settle in new party, CPI (M) and it fought elections in West Bengal and came in power by forming coalition 'United Front'. This ridiculed many party members and among them were Charu Mazumdar, Kanu Sanyal and Jangal Santhal.

Naxalbari Incident

Naxalbari, a village near Siliguri North West Bengal, became infamous in 1967 as it revived left wing extremism in India. Charu Mazumdar was active leader of the area and was mobilizing peasants against state for an armed conflict. On the other hand there were repetitive incidences of Class conflicts between peasants and zamindars. One such conflict escalated and zamindar was expelled from his land. After this police came to his rescue and was surrounded by about thousand peasants armed with bows, arrows, lathis etc. One Police officer was killed. Police force few days after responded with brutal force and 9 women and 2 children were killed. This was sanctioned by united front government of whom CPI was part.

In response revolutionary leaders fled the area and declared armed struggle against state of India. They formed a new party Communist Party of India (Marxist-Leninist) in 1969 and this was motivated and influenced deeply by Communist Party of China. In fact, Charu Mazumdar wrote 8 documents which was sort of road map for his group. He sent these documents to China to be approved by Mao Zedong.

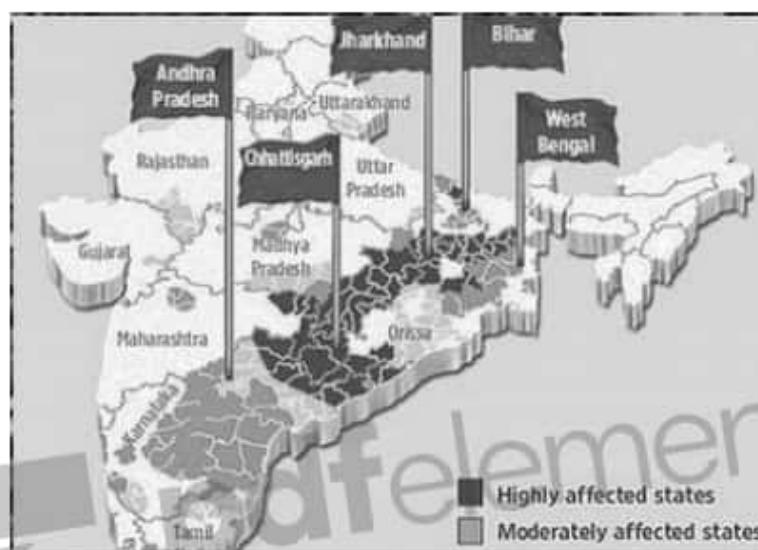
This incident fired the imagination of Bengali Youth and there was popular support for Charu. Many university students joined the organization and became part of its different forms of front organizations, which they use for propaganda.

In 1972, Charu was caught and he died under custody. After this, movement went underground. Heavy state response kept violent incidents under control in 1970's but it got push in 1980's. This time it was from Andhra Pradesh. Actually, in 1967 itself movement also started in Srikakulam, Andhra Pradesh. Here revolutionaries tried to mobilize tribals into armed militias called 'dalams', by inciting them against landlords, money lenders and government. They resorted to 'annihilation of class enemy' under which people those represented state i.e. government servants, Forest officials and other oppressive characters such as money lenders and landlords, were

to be identified and killed. They killed about 100 such targets and this was followed by arrest of its main leaders which brought movement to standstill.

In late 1970's Kanu Sanyal was released and in 1980 K. Seetharamaiah founded **People's War Group**. Original CPI (ML) by this time has changed name to **Maoist Communist Center.** It was seen that in 1990's popular support to Maoist movement waned in backward districts. This coupled with disintegration of USSR and diversion towards market economy by China was a big blow to ambitions of Indian left wing.

These two parties/groups merged in 2004. With this, they gave a statement about their aim. It states that the Communist Party of India—CPI (M) is representative of the Indian proletariat (working class/labor) and its ideological foundation is Marxism-Leninism-Maoism. Its political objective is overthrow of what it calls the semi-colonial, semi-feudal system under neo-colonial form of indirect rule, exploitation and control in India of the oppressed masses. This struggle will be carried out through armed agrarian revolutionary war i.e. the **Protracted People's War** with area wise seizure of power. This is old Maoist principle under which base is made in rural areas and more and more people are gradually brought into its fold. Overtime, influence will be extended to urban areas.

Current Situation

Naxalism has spread to 17 states in India, including Assam, Andhra Pradesh, Bihar, Chhattisgarh, Jharkhand, Karnataka, Madhya Pradesh, Maharashtra, Orissa, Uttar Pradesh, West Bengal to name the few main ones, affecting nearly 185 out of 602 districts.

With established base areas in Dantewada and Bastar districts of Chhattisgarh, the movement has shown no signs of abating there. Reports indicate that Naxal armed underground cadres number around 15,000 men and women, with 12,000 firearms, and an unarmed cadre strength of nearly 200,000.

Nearly 60 per cent of the armed contingent of the Naxalites is in Northern Chhattisgarh and Jharkhand. In fact, according to the 2008 Internal Security Report, Naxalite violence in Chhattisgarh and Jharkhand was as high as 58. 56 per cent and most of the casualties were due to the use of landmines and Improvised Explosive Devices (IEDs) in these states.

Why Naxalites are concentrated in Chhattisgarh and Jharkhand? This is because they run extortion network under which main targets are mining companies and firms. These companies or sites of work are in far off locations which make them easy to be compelled. Also, parts of these sates are quite socio-economically most backward. So, it turns people more vulnerable to their ideologies. Lastly, they give employment to downtrodden people and pay them out of this extortion money.

Stated Purpose of Naxalite Movement

The Naxalites state their main political purpose as establishing an alternative state structure in India by creating a "red corridor" in Naxalite-affected states, stretching from the border of Nepal to central India to Karnataka in the south through violent struggle. This requires local support, Naxalite rebel leaders take up causes like protecting people's rights of Jal, Jangal and Jamin (water, forest, and land) and providing justice through their committees/ kangaroo courts. Local support is crucial for the Naxalites for cadre recruitment, intelligence, logistics, and territorial control.

Strategy

Their Strategy as per writings of Mao Zedong should be –

1. Organization, consolidation, and preservation of regional base areas situated in isolated and difficult terrain.
2. Progressive expansion, which includes attacks on police stations, sabotage, terror tactics, elimination of persons with alternate viewpoints.
3. Destruction of the enemy through conventional battles and capture of power.

In initial phases they wage guerilla warfare and inflict surprise attacks. This is to make enemy weaker and project their claim over an area. This is also used by them to make common people under their influence believe that state is not all mighty and it is possible to defeat the state. They keep a strict vigil on people under them and suspected detractors or people with different views are brutally killed or tortured.

This strategy is long one, and they believe that it will take decades to achieve their objective. Till they prefer to silently strengthen their network and build capacity. Some leaked official documents of CPI (M) suggest that they plan to bring down Indian State by 2050 or 2060. Obviously, this is outright impossible, but we'll have to agree that they can inflict substantial damage and State's responsibility and focus is to minimize this damage. Perhaps they know that under present designs and capacity they can't withstand might of state, so any aggressive act can possibly uproot them.

It is said that, Indian forces has so far just faced 5% of Maoist cadres, that too of second rung. They possibly have more sophisticated, better armed and trained elite force, which they are yet to brandish. Further, it is suspected that they might be receiving some support from retired armed forces personnel or some foreign powers. This is apparent because many documents has been seized which assimilates procedures and practices adopted by professional state armed forces. One arrested Maoist commander also revealed that they have elaborate training programme in place which stretches from 4 to 6 years.

Worse is that they are amicable to any anti-India force which serve their purpose. Whether they are terrorist organization, organized crime mafias, Human/animal traffickers, smugglers or any foreign state enemy of India, all have some or other nexus with Maoists. They can make use of counterfeit notes, provide passage to illicit materials, give refuge to anti national elements and carry out contract killings to get what they want in return. This way they can arrange for money or modern weapons.

They have openly declared their support for Kashmir and North east separatists. Linkages between the Naxalites and the People's Liberation Army in Manipur (PLA) came to light when PLA and Maoist cadres were arrested in Delhi in 2011 while making elaborate plans to form a "strategic united front" with the Naxalites in India. Following their arrest, it was also revealed that the PLA had trained and armed the Naxalites in Jharkhand and Orissa in 2009 and 2010 respectively. There were plans to train Naxalite cadres in the PLA camps in Myanmar in 2012.

In normal course they take up social and economic causes against the government, without being identified as naxalites. They try to obstruct every developmental project. Any mishappening and state negligence is big opportunity for them to provoke people. For e.g. recent tragedy with 13 women in sterilization camps in Chhattisgarh or poisoning through Mid-day meal food, will be used by them against state. Further, they few years wowed to obstruct creation of any Special Economic Zone in India, which they consider foreign enclaves in India which are made to grab agri lands. Singur protests in West Bengal few years back is another example. Also, they are believed to have support of anti-dam protestors of Assam and Arunachal Pradesh.

(The general concern of police sources is that the anti-talk faction of the ULF A may try to establish strong linkages with the Naxals and provide them with arms from its base in Myanmar and China. The small arms network is one of the strongest in the Northeast running all the way from Thailand, China, and Cambodia via Myanmar to Manipur and Nagaland.)

Having said this, they operate their own medical and education services under the areas controlled by them. Similar confidence building exercise by state is not liked by them, so they have in past attacked government schools and hospitals.

Recruitments by Naxals

Naxals often use coercion for employing new cadres. They introduced compulsory service of one member from every Adivasi family. This caused much resentment in Adivasis which decreased their influence. Once on rebellion by people against this practice, 70 villagers were killed by Maoists.

Apart from this they use every possible mean including political indoctrination, promises of better future, remuneration, alliances with other violent groups etc.

Ethnical, tribal and religious identities also propel recruitment. Shared identities and social networks work to a great extent in collaborative efforts. Also some rich recruits who are highly committed to ideology become financer of their operations.

Front Organizations and Urban Presence

Maoists have ultimate objective to capture the cities and Mao in a statement said that this is not possible without 'adequate work' on ground in urban areas. This is part of long term strategy and for this Maoist have Front Organizations active in Cities.

There have been traditionally, underground urban networks, providing logistic supplies to interior bases, providing shelter in case of medical emergencies etc. But these front organizations keep alive anti state ideology in the media. They condemn government desperately on every stem. They try to mobilize working class against employers and government. They may form underground networks through which they can attempt to sabotage state security by any possible means.

The strategy for urban areas of the country includes mobilization and organization of the working classes, building a Tactical United Front (TUF) of classes similarly placed to the working classes and military tactics involving sabotage actions and select assassinations by 'action teams'.

The organisations with which the Maoists have formed the TUF include the Revolutionary Democratic Front (RDF), the People's Democratic Front of India (PDFI), the Committee against Violence on Women (CAVOW), and the Committee for the Release of Political Prisoners (CRPP), among others.

Time and again, Maoist Sympathizers are arrested from Delhi and found to be aiding activities of the Maoists.

Where's the fault of government?

Mao Zedong said that –

"Without a political goal, guerilla warfare must fail, as it must if its political objectives do not coincide with aspirations of the people and their sympathy, cooperation and assistance cannot be gained."

This comes out to be apt statement if we see Indian experience. Movement exists only in those districts where there is administrative and developmental vacuum. If India's growth had trickled down a bit to these areas, then story would have been altogether different.

As a development strategy the government has stressed on the urgent implementation of development projects/policies of the government including

1. Backward Regions Grants Fund –
   it is designed to redress regional imbalances in development. The fund will provide financial resources for supplementing and converging existing developmental inflows into 250 identified districts. This aims at filling local infrastructural gaps, strengthening local government institutions and building mechanisms for professional help to these local bodies.
2. Panchayat (Extension to Schedule Areas) Act of 1996 (PESA)

   This act (PESA) exempted scheduled areas (schedule v) from certain provisions 73rd amendment. It also modified certain other provisions. Through PESA certain powers are given to gram sabha, which under 73rd amendment might not have been available to them (because of state's discretion).

3. National Rural Employment Guarantee Programme and
4. The Schedule Tribes and other traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006 – In short **Forest Rights Act**

   The law concerns the rights of forest-dwelling communities to land and other resources, denied to them over decades as a result of the continuance of colonial forest laws in India.

   This act recognized rights of tribals over minor forest produce. Recently, Forest Minor produce was also covered under Minimum selling price regime.

5. New **land acquisition act** which includes, consent, enhanced compensation, social impact assessment and Rehabilitation & Resettlement of displaced.

With all these efforts in place, reports have indicated towards poor implementation and translation of these schemes to the grassroots, primarily due to conflict prone environment.

It should be noted that Maoist too has their agenda in form of a manifesto, which include almost all those things which State includes, such as addressing caste based discrimination, protection of religious minorities, No displacement by big projects etc.

In order to secure better co-operation, **Chief Minister's Conference on Internal Security** is being held since 2009. There has been Prime Minister Rural Fellowship Scheme under Ministry of Panchayati Raj for affected areas. Also, infrastructure spending in these areas is also being promoted, for ex. by Pradhan Mantri Sadak Gram Yojna

Counter operations by Center/State government

Maintenance of law and order is domain of state governments, yet central government has deployed troops of CRPF in these areas. These troops are attached to police station or to district police. They don't have specific job assigned to them and hence doesn't have autonomy. They just act as support system to state police. Also, centre has deployed there CoBRA – Commando Battalion for Resolute Actions are also deployed. These are elite forces specializing in guerrilla and jungle warfare

This has time and again created chain and command problems. There have been ego problems and confusion between operations of two forces. Further these forces are commanded by Inspectors who are in their 50's and don't have any experience of similar operations, knowledge of terrain and intelligence support.

Recently about 14 members of CRPF were killed in Maoist attack and this was partially due to lapses on part of troops as they compromised protocol. This caused much anguish in public and there was some clamor demanding involvement of army. While army is involve in training of CRPF and State police troops, yet it is not involved in operations.

Experts are overwhelmingly against involvement of Army because of following reasons:

1. Army is option for the last resort. Currently problem is not lack of physical capacity of our police/paramilitary forces, but intelligence support is certainly lacking. In absence of this Army will end up achieving very little and deterrent aura of Army reservoir will be lost.
2. Further, Maoist will use this deployment and some associated developments as deliberate abuse of power by government against poor tribals. This may earn Maoist sympathy of tribals.
3. Our Army is already over stretched and if we start using it internally, our frontiers will be quite vulnerable. This we can't afford as we know nature of our neighbors.

It may be asked that, then why AFSPA is implemented in J&K and North East areas, but not in Maoist affected area? This is because they already are on international borders and anti-state elements there are actively being supported by foreign power.

Grey Hound Police

The **Greyhounds** are an elite commando force of Andhra Pradesh, India created to combat left wing extremists. It is considered the best anti Naxalite force in the country, even above the CRPF's CoBRA which has more men, budget and better arms than the Greyhounds. Greyhound is a simple but effective organization and recruits the best of the best from the Andhra Pradesh Police. The Force is also known for its guerrilla approach and its functioning in the field, which is near similar to that of the Maoists. Greyhound commandos often exclaim that their strength does not lie in them being a special force with special training, but it lies in the fact that it is more of a guerrilla force than a special force. The commandos of Greyhounds undergo rigorous training and have a strict day to day combat regime. They are highly paid, motivated and well-armed.

Operation Green Hunt

It was the name used by the Indian media to describe the "all-out offensive" by government of India's paramilitary forces and the state's forces against the Naxalites. The operation is believed to have begun in November 2009 along five states in the Red Corridor.

Recent attack on CRPF battalion is said to be in retaliation against this operation.

Salwa Judum

So called People's movement was named Salwa Judum, to mean, "Peace hunt" in the local Gondi tribal dialect. The movement was launched by a few villagers angered by Naxal interference in the local trade of tendu leaves (used for making bidis).

However, later on, it was alleged that maintaining law and order in Dantewada and Bastar was outsourced to the Salwa Judum cadres, some of them as young as 15–16 years in age. Some 5000 such cadres were made Special Police Officer s (SPOs), given a rifle each and paid Rs 1500–2000 a month. Poorly trained, ill equipped and immature, some of the Salwa Judum cadres themselves looted many tribal villages. It resulted in civil war like situation in these regions. Last year, Supreme Court ruled that this movement id unconstitutional and only state has responsibility of maintaining law and order.

Peace Talks with Maoists and cease fires

In 2004, Andhra Pradesh government entered into peace talks with the Maoist. Maoist showed unwavering stand and put up strange conditions, like they should be allowed to wield arms wherever they like, state should call back troops from their areas etc. It was clear that Maoist Plan for ultimate overthrow of Indian state is nonnegotiable. They just wanted to buy time to strengthen themselves. During this time their Leader (kishenji) addressed huge rally in Hyderabad (attended by approx. 1.5 lakh people). Soon after this, merger of two parties (MCC & PWG) surprised everyone.

Again in 2009, Home Minister P. Chidambaram called for ceasefire and peace talks, Maoist first accepted cease fire, but within few hours there was an attack on paramilitary battalion, killing them, which belied all expectations of peace with Maoists.

Surrender Policy

Naxal-affected states have also announced surrender policies. The Jharkhand government offered Rs 50000 to surrendered Naxalites plus a monthly allowance of Rs.2000,one acre of agricultural land, and educational and health benefits to their children. The Chhattisgarh government offered up to Rs.3 lakh for weapon surrender. The Orissa government announced Rs. 10000 for surrender, Rs.20000 for arms surrender, and Rs 2 lakh of bank loan without interest for two years.

But there is no effective intelligence mechanism to identify Naxal cadres .Often, tribal youths surrender as Naxal cadres; many of them even join the Naxal movement to reap these benefits.

Further it is alleged that Police forces pressurize (even coerce) those who surrendered to reveal information, or to join counter-Naxal operations like Salwa Judum. This demotivates rebels who want to surrender.

Lives claimed by Naxalism have come down drastically in recent years due to better center state cooperation. Recent Chhattisgarh and general elections were concluded peacefully and districts of Bastar and Dantewada too voted in reasonably good numbers. This indicates situation is under control for the time being. But as explained, government can't be complacent until it is uprooted completely. There are still surprise attacks where they inflict substantial damage at our paramilitary forces. Their vigour of attack doesn't suggest that they are demoralized, but it appears that they are waiting for the right time to raise their head. A time when

Indian state is weak or engaged in external conflict, could be most opportune for them. Wait and patience is inherent in policies of Mao. So it is imperative that government instead of being reactionary goes after them proactively. But it has herculean challenge of doing it in democratic way.

It is obvious that there is (and should be) two pronged approach to counter it, one at ideological level and other at physical level. In former case, good governance by government and delivering good results in fields of Education, Health and overall standard of living will be instrumental.

7.ROLE OF EXTERNAL STATE AND NON-STATE ACTORS IN CREATING CHALLENGES TO INTERNAL SECURITY

Internal security for any country is of prime importance. If the internal security issues are undertaken effectively, rebellion by the external forces to that extent becomes more difficult. Unfortunately, the rise of quarrelsome politics based on sectarian, ethnic, linguistic or other divisive criteria, is mainly responsible for the many communal and secessionist movements thriving in India. The presence of hostile neighbours allows the internal conflicts to get external support, which includes money, arms and sanctuaries. The vested interests exploit these conditions to pursue their own schema.

In strong political system and a developed economy, conflicts between the various group identities are kept under surveillance as in due course they get assimilated into the national identity. But in India, it is not possible because the partition and the colonial rule have still not fully rehabilitated. Furthermore, the dependence on the government by a large section of our people for their survival sharpens these conflicts among them. The democratic institutions and the state structures are still not good to fully synchronise these conflicts in a peaceable manner. Violence blow up when conflicting interests cannot be consensually reconciled. The hostile external forces, taking advantage of this situation through subversive propaganda, further highlight these conflicts. They give material and political support to worsen this sense of grievance to such an extent that a small minority are willing to become tools in their hands to undermine the stability and security of the nation.

Transnational organized crimes, drug trafficking and international terrorism, are labelled as "non-state actors". These are, today, major challenges for internal and international security and strength.

In present situation, India faces manifold security challenges. India's security concerns is its 'internal security' and it is a major national security challenge. Among many indeterminable factors of India's security system, internal security is considered as one of the principal fundamental aspects.

Awkwardly, in current scenario, there is an obscuring distinction between internal and external threats. Some experts debated that "India does not face an external

threat in the conventional sense" but only internal security threats from external sources. These external sources, consist of both state and non-state actors, combined with those anti-state forces within India, have made the situation more intricate. All over the world, few countries are placed in an unfavourable, troubled and uncertain security environment as India is. External sources of threats to India's internal security spring from almost all countries of its neighbourhood.

According to famous economist of Maura times, Kautilya, a state could be at risk from four types of threats such as internal, external, externally-aided internal and internally-aided external. Among all threats, the internal threats should be tackled immediately for internal troubles, like the fear of the lurking snake, are far more serious than external threats. Thus, the most dangerous opponent is the enemy within. However, external state and non-state actors both have played an active role to disturb internal security and raise numerous problems in India.

India is currently facing four major threats such as
- Separatism in Jammu and Kashmir
- Insurgency in North East India
- Left Wing Extremism
- Terrorism in the Hinterland.

Out of them, the first and the last are a direct appearance of Pakistani influence, which includes the ISI and Pak military. Recently, these two threats are more serious due to rise of ISIS in Middle East. The rebels in north east get direct and indirect support from neighbours of India around its permeable north east border. The left wing extremism has direct and indirect support from Nepal, China and other countries of South East Asia. Traditionally, India has border clashes with Pakistan, China and Bangladesh. The problem with India is that it is situated on the epicentre of terrorism and dealing with so many hostile neighbours, all at once. India had direct wars with our neighbours in 1947-48, 1962, 1965, 1971 and 1999.

Major grounds for India's security circles include Nuclear Competences of China and Pakistan Military assertiveness and String of Pearls strategy of China Pakistan's military rule beneath the civilian government, Anti-India sentiments in Nepal and Bangladesh, Uncertainty of Sri Lanka in Tamil cause and fishermen issues, the anxiety of Bhutan to move closer to China, illegal immigration from Bangladesh to create cultural issues in North East.

Therefore, the entire matter can be divided into following:
- Role of state and non state actors in Pakistan

- Role of state and non-state actors in China
- Role of state and non-state actors in Nepal
- Role of actors in Bangladesh.

Role of state and non-state actors in Pakistan:
It is evident that there is covert and overt threat from Pakistan to India's internal and external security system. Since its origin, India has fought four wars in 1948, 1965, 1971 and 1998 with this rogue country. Resulting to its military inability to confront with India in direct war, India is facing low intensity conflict in J&K assisted and sponsored by Pakistani military, in the North-East and through support to various fringe extremist groups within the country. India also face huge economic challenges due to the fake currency rackets. Pakistan is one of India's main concerns both on external and internal security fronts. Due to its continued strategic partnership with China, it can stretch Indian armed forces capabilities in the Eastern sector also. The Chi-Pak link has given rise to external concerns such as modernization plans of Karakoram highway, development of Gwadar as a naval port and covert assistance in Pakistan's nuclear and missile program.

The various state and non-state actors in Pakistan include:
Inter-services Intelligence and Pak Military Islamic terrorist groups like the Al-Qaeda, Lashkar-e-Toiba, Harkat-ul-Jihad Islami, Jaish-e-Mohammad, and the Pakistani Taliban along with various other Jehadi Tanjims. The surreptitious activities of these apart from terrorist attacks in various parts of the country, include training and facilitation to armed insurgents by ISI in various training camps in Pakistan. Apart from Kashmiri militants, ISI has in past and present trained the Sikh Separatists also. Recently, according to union government, the ISI has been trying to revive the Sikh Militancy to perform terrorist attacks in Punjab and other parts of the country.

State and Non-State Actors in China:
Conventionally, China has provided financial support, arms and sanctuaries to Naga, Mizo and Meitei extremist's right since the British Period. The military encroachments and conflict of 1962, India was defeated and became psychologically weak. Since then, China has been astutely following a policy of strategic

containment of India by regional coalitions and arming India's neighbours Myanmar, Bangladesh and Pakistan.

As far as internal security is concerned, China's interest lies in North East as well as the Left Wing Extremism. The Nagas were the first to approach Beijing, but China made best use of it. Other groups such as MNF, ULFA, PLA, ATTF and NDFB followed. However, it cannot confirm that the linkage was unilateral. It was a relationship of convenience and an alliance of opportunism between China and Indian militant groups. Both Issac Swu and Muivah have been visiting the Chinese embassy officials in Geneva and there are reports of Chinese offer of basses in Yunan. The Maoist movement got philosophical, moral, financial and intellectual support from China.

State and Non-state actors in Nepal:

India and Nepal are good neighbours and share an open border with free exchange of people and currency across the borders. The CPN (Maoists) have become difficult political power (non-state actors so far, but state actors now) and this brings new implications for India's internal security mainly in view of their known linkages with Indian Left Wing Extremists. Furthermore, India's dominance in Nepal is not remains the same as in past as the Maoists have been continually upping the ante against India, accusing India of invoking in internal Nepali affairs. Consequently, Nepal can significantly add to India's Maoist threat by supporting the rebels in the red corridors of India. Thus, the clarifying political and security scenario in Nepal would have to be closely monitored.

Role of various players in Bangladesh:

Trans-border relocation from Bangladesh is a major issue in Assam and other areas of the North East.

It is well recognised that Bangladesh refugees create communal and ethnic tension. It was well proved by the Assam agitation and successive events. There are estimated to be 15 to 18 million illegal Bangladeshi immigrants in India, who expanded their network to all the North Eastern States with majority of them being in Assam. In some states, these illegal immigrants have turned the majorities into minorities. The invasion is likely to continue unless checked and those already identified are deported. Their wrongdoing into land and providing cheap labour is a cause of social

and economic insecurity for local communities and a cause of tension and violence. Such problems are intense. India needs to make strong policies to curb immigration.

The electoral politics since 1980 have resulted in diffusion of both the state and politics, the institutions of governance have been diluted and politics have lost their philosophical and moral anchorages. While on one hand, it has led to increase of the social base of politics, on the other hand, due to corrupt politics, it has resulted in politicisation and exacerbation of all problems. Democratic freedom and electoral politics have led to agitation and turbulence.

The exploitation of diversities has caused breakdown of the cohesiveness of the society, created uncertainty of cultural identity, stimulated religious revivalism in its fundamentalist form, intensified ethnicity and broadened the gap between the sub national groups and nationalism. The assurance of the distortion of the system is political pragmatism. In the economic and developmental field, it has resulted in bewilderment, subversion of the system, permissiveness and malpractices with corruption as the natural outcome.

Information Technology has revolutionized conflict and in the internal security area, it has provided means to the underworld to increase their reach for criminal activities without direct physical involvement. Pak ISI has exploited it by linking up with the Bombay underworld. India's responses have to be quicker and based on the developing technological inputs. This will require updating educational levels in the security forces and developing a technological temper. Likewise, liberalisation of economy has resulted in prominence of economic disparities as benefits have not reached to the masses. This is bound to increase social and economic tensions.

To summarize, there are several challenges to India's internal security. Most external threats originate from a troubled boundary dispute with China and ongoing cross-border jihadi terrorism in J & K sponsored terrorism, supported by ISI and Pakistan-based Islamist fundamentalist organizations such as Lashkar-e-Taiba and Jaish-e-Mohammad who, in turn, are inextricably linked with international jihadi groups like Taliban and Al Qaida. Threat from Bangladesh undertakes serious magnitudes since it became a base for northeast rebellious groups like ULFA and Naga factions. In order to handle external threats to security, it is important to observe internal threat. The opponent within has to be recognised. Numerous socio-economic and religious conflicts within Indian society exist but forging unity in a diverse society.

8.SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS

Governments of numerous nations make huge investment and provide good support for the border security. Still, border and maritime security continues to present challenges to governments around the world. The proper management of borders presents many challenges and includes coordination and concerted action by administrative, diplomatic, security, intelligence, legal, regulatory and economic agencies of the country to secure the frontiers and sub serve its best interests. With a continent of sub-continental proportions, India occupies a major strategic position in Southern Asia and governs the northern Indian Ocean with a coastline that is 7,683 km long, and an Exclusive Economic Zone that is over two million square km in size. India's land borders exceed 15,000 km which it shares with seven countries including a small segment with Afghanistan (106 km) in northern Jammu and Kashmir (J&K).

It has been established by security experts that good management of borders is extremely important for national safety. In India, borders are extended to different portions which create many issues and these issues must be appropriately addressed. These problems have become intensified currently with Pakistan's policy of cross-border terrorism, along with its strongly hostile anti-India publicity designed to misinformed and power the reliabilities of the border population. The increase of cross-border terrorism, targeted to weaken India, also pose main challenges for border management strategy. The Department of Border Management was created in the Ministry of Home Affairs in January, 2004 to pay focused attention to the issues relating to management of international land and coastal borders, strengthening of border policing and safeguarding, creation of infrastructure like roads, fencing and flood lighting of borders and implementation of Border Area Development Programme.

The term border management must be understood in its broadest sense and should infer co-ordination and concentrated action by political leadership and administrative, diplomatic, security, intelligence, legal, regulatory and economic agencies of the country to secure Indian boundaries the best interests of the country. From this perspective, the management of borders offers many challenging problems. Numerous factors like globalisation, media uprising and technological development in various fields have hugely impacted the border management

framework. Now more comprehensive planning is needed to attain peace and progress on borders. Geocenterality of India and the fear of the smaller neighbouring States of India's size, economic resources and military strength has impacted on communal relations. India faces military and non-military threats from all countries with land borders. Land borders with Pakistan and Bangladesh have observed rapid security affecting changes. Borders with Mayanmar and Nepal are also causing serious concern. Pakistan and India have fought four wars over the issue of J&K (Sanajai Singh, 2005). The problems continue and proxy war unchecked to wrest J&K continues. Without peaceful borders with its neighbours, India can hardly play its appropriate role in global matters at this time of seminal global change. Currently, there are many problems on the border management regardless of the security measures in order to combat cross border terrorism.

The theory of border security has changed with the increasing vulnerability of the coastline and also of the airspace. With gradual expansion and strengthening of security, the lawbreaker is already on the look-out for soft gaps, either on the land or along the coast and if need be, from the air. The offenders, with unprecedented money power, access to modern technology, organisational strength, manoeuvrability and scope for strategic alliances with other compatible groups, can choose their theatre of action for surprise attacks. While land borders have from time to time received Government's attention mainly because of the wars with Pakistan and China and the problems of insurgence, illegal migration from Bangladesh and smuggling actions. Rebellious groups in various parts of the country are receiving foreign support and inspiration. Illegal penetration and smuggling of arms and explosives, narcotics and counterfeit currency are persistent problems. The absorbency of borders in many parts, makes the task of the anti-national forces much easier. All this activities emphasises the need for extreme vigilance on the borders and strengthening the border guarding militaries.

In India, when reviewing thoroughly management of borders, the Kargil Review Committee had concerned about land borders. The Group of Ministers (GoM), realized that the scope of such a review should be broader and apart from including the land borders, should also include management mechanisms designed to safeguard the safety of coastal areas and airspace. By doing this exercise, the GoM was assisted by a multi-disciplinary task force. Based on the report of the task force and the ensuing deliberations, the GoM made a series of recommendations designed to better manage our borders, coastline and airspace. Some of the major issues bothering the management of borders include maritime boundaries. Maritime boundaries are still undefined and much of land borders are not determined on the ground. The disputed and unsettled nature of boundaries has made them a source of

tension with their policing much more problematic. Since most of Indian borders are man-made artificial boundaries and not based on natural features such as rivers and watersheds, they are very permeable and easy to cross. Diversity of forces on the same borders has unavoidably led to the lack of accountability as well as problems of command and control. Border Guarding Forces must have to be distinguished from central police organisations. They need to be properly strengthened both in terms of equipment and manpower.

The forces antagonistic to India have tended to occupy the vacuum created by inadequate reach of the national media. To fight terrorism and revolt, security forces are called upon to take tough measures. These measures may sometime cause trouble and infuriation to the local people. This sense of dissatisfaction is misused by hostile elements to create a feeling of ill will against the security forces and the Government. When media releases information at appropriate time, it would help in combating such unenviable publicity of the elements hostile to India. Due to the sensitive nature of their responsibilities, the interaction of the bureaucrats of the security agencies and security forces with the media has necessarily to remain limited. Though, specialized officers, properly equipped and trained may communicate information to the media. The concept of Village Volunteer Forces helping in border management has a great deal to commend itself and has worked with huge success in areas where it has been tried so far.

Information about the length of India's land borders with its neighbours:
Bangladesh: 4,339 km (4,351 km as per MoD2).
Bhutan: 605 km (700 km as per MoD).
China: 3,439 km (4,056 km as per MoD).
Myanmar: 1,425 km (1,643 km as per MoD).
Nepal: 1,690 km (1,751 km as per MoD).
Pakistan: 3,325 km (3,244 km as per MoD).

Additionally, India has a land border with Afghanistan as well. Nevertheless, currently, the area bordering Afghanistan falls in the Northern Areas of Pakistan Occupied Kashmir.
Due to the inclination of India's neighbours to exploit India's nation building problems, the country's internal security challenges are intricately connected with border management. The challenge of coping with long-standing regional and boundary clashes with China and Pakistan, combined with permeable borders along some of the most difficult landscape in the world, has made tremendously effective border management compulsory. In spite of several border wars and conflicts, India's borders continue to be operated by huge number of military, para-

military and police forces, each of which has its own beliefs, and each of which reports to a different central ministry at New Delhi, with almost no real co-ordination to manage the borders.

Country	Length of border (in km)
Bangladesh	4096.7
China	3488
Pakistan	3323
Nepal	1751
Myanmar	1643
Bhutan	699
Afghanistan	106
Total	15106.7

External threats to India's security are not the only border management issue to be dealt with at present by the national security apparatus. India's rate of growth has far outperformed that of most of its neighbours which has created peculiar problems such as:

1. Mass immigrations into India.
2. Augmented cross-border terrorism.
3. Penetration and ex-filtration of armed militants.
4. Emergence of non-state actors.
5. Link between narcotics and arms smugglers.
6. Unlawful migrations.
7. Left-wing radicalism.
8. Separatist movements aided and abetted by external powers.
9. Establishment of madrasas, which could result in security hazards.
10. Smugglers, drug-traffickers are often in association with local offenders, lower rung political leaders and police officials.

These type of situations worsen the challenges of border management and the border guarding agencies face more complex problems. It is obvious that poor border management inexorably results in a volatile internal security situation in the Border States of the nation.
The engagement of various forces results in problems of command and control as well as the lack of accountability for violations, poor intelligence and incompetent handling of local sensitivities.

Staffing the Line of Actual Control with China:

The Line of Actual Control (LAC) with China is a lively example of the lack of synchronisation in border management. The western sector of the LAC in Ladakh and Himachal Pradesh and the central sector along the Uttrakhand border are staffed by some Vikas battalions of the Special Frontier Force which reports to the Cabinet Secretariat and the Indo-Tibetan Border Police that is a Ministry of Home Affairs police force, correspondingly. Infantry battalions of the Indian Army man the Sikkim border and units of the Assam Rifles (AR) man the Arunachal Pradesh, Nagaland, Manipur and Mizoram borders. The Assam Rifles is a para-military force under the Ministry of Home Affairs that is officered mostly by regular army officers. Its battalions have been placed under 'operational control' of local army formation commanders. Though the responsibility is that of the army, the Assam Rifles battalions given to the army for border manning operations are not directly under its command. This plan is not favourable for developing a professional relationship between the commanders and their juniors.

The Western and Other Borders: In the west, the intact border with Pakistan is managed by the BSF except the Line of Control (LoC) in Jammu and Kashmir (J&K). The LoC is the duty of the army with some BSF battalions placed under its operational control. Since the LoC has been mostly active on a daily basis, particularly since the early 1990s, this is considered as proper arrangement. On the LoC, the prime operational responsibility is to safeguard its physical integrity against violation by the Pakistan Army. The army's secondary responsibility is to lessen trans-LoC penetration by armed mercenary terrorists usually aided and abetted by the Pakistan Army and the ISI.
Since last fifty years, the Kashmir conflict is there, the two armies were betrothed in a confrontation with loss of deputed army men and property. An informal cease-fire has been in place all along the LoC, including at the Actual Ground Position Line (AGPL) along the Saltoro Range west of the Siachen Glacier, since November 25, 2003. Though the LoC is no longer 'live' as small arms fire, machine gun and mortar fire have almost totally stopped, penetration from POK remains at reduced rates.

The border with Nepal was almost not attended till very recently as Nepalese peoples have free access to live and work in India under a 1950 treaty between the two countries. Since the outbreak of a Maoist rebellion in Nepal efforts have been made to progressively step up vigilance along this border as India fears the southward spread of Maoist ideology. The responsibility for this has been entrusted to the Sashastra Seema Bal (SSB), erstwhile Special Security Bureau.

Management of Indo-Pakistan border:

India has command land of 3,323 Km (including Line of Control in Jammu & Kashmir sector) with Pakistan. This border is attached with the States of Gujarat, Rajasthan, Punjab and Jammu & Kashmir. Border Security Force (BSF) is the Border Guarding Force at Indo-Pakistan Border. Major Initiatives for effective Border Management:

1. Fencing: In order to stop illegal immigration and other anti-national activities from across the border, Government of India has sanctioned erection of fencing along Indo-Pakistan border.
2. Floodlighting: Government of India has also taken up floodlighting works along the Indo-Pakistan border for close vigil, particularly in the night hours

Management of Indo-Bangladesh border:

India has common land of 4096.7 Km with Bangladesh. The entire stretch include plain, riverine, hilly/jungle and with hardly any natural problems. The area is densely populated, and the cultivation is carried out till the last inch of the border at many stretches. Border Security Force (BSF) is the Border Guarding Force at Indo-Bangladesh Border. India's border with Bangladesh has a strange problem of 'Enclaves and Adverse Possessions'. "There are 111 Indian enclaves within Bangladesh and 51 Bangladeshi enclaves in India." Thirty-four tracts of Indian land are under the adverse possession of Bangladesh and 40 pieces of Bangladeshi land are in India's adverse possession. Though the Land Border Agreement of 1974 has provisions for the settlement of the issue of adverse possession, it has not been applied so far as the problem is administratively sensitive. The border guarding forces are left to deal with the day-to-day problems that are bound to be thrown up by such territorial complexities. It is necessary that political leadership must invest time and effort to resolve this sensitive issue, unseemly clashes that do no credit to either side will continue to occur and pamper relations between the two nations. Major security issue with Bangladesh is migration. Border management problems such as smuggling, illegal migration, insurgency, trafficking of women child and the

construction, repair and maintenance of boundary related structures are addressed through border coordination conference between the border security force and Bangladesh rifle (Mahendra Gaur, 2005).

Major steps taken by government for Effective Border Management:

1. Fencing and Roads: To avert illegal immigration and other anti-national actions from across the border, Government of India has sanctioned erection of fencing/roads in two phases, along IndoBangladesh border.

Management of Indo-Nepal border:

The vigorous nature of the problems about borders management is brought out by the manner in which the sensitivity of India-Nepal border has changed over a period of time. This border, which has been an open one, was once nonviolent and trouble-free. Nonetheless, with the increasing activities of Pakistan's Inter-Services Intelligence (ISI) in Nepal, the nature of the border has changed absolutely. In order to check anti-national activities on the India-Nepal border which is the open and absorbent border and to improve the security along this border, 25 battalions of Sashastra Seema Bal (SSB) have been deployed as the Border Guarding Force (BGF) on this border. All the 450 Border Out Posts (BOPs) have been established on Indo-Nepal border. Bilateral mechanisms in the form of Home Secretary-level talks and Joint Working Group at the level of Joint Secretaries exist between the two countries. Additionally, there is a mechanism of Border District Coordination Committee Meetings between the district officials of the two nations. These mechanisms serve as platforms for discussing issues of mutual concern like containing cross-border crimes, smuggling, and situation arising out of terrorist activities, at national and regional/local levels correspondingly.

Management of Indo-Bhutan border:

India shares a 699 Km long border with Bhutan along Sikkim, West Bengal, Assam and Arunachal Pradesh.

Deployment of border guarding force: To increase the security environment along this border, 12 battalion of Sashastra Seema Bal (SSB) have been deployed as the Border Guarding Force on this border.
Indo-Bhutan group on border management and security: A Two-sided mechanism in the shape of an India-Bhutan Group on Border Management and Security has been regularly meeting. This mechanism is useful in assessing threat perception to the two

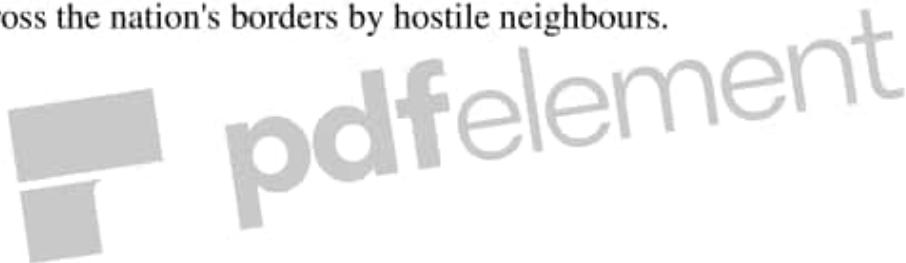
countries from groups attempting to take advantage of this open border and in discussing ways to improve the security environment in border area.

Management of Indo-Myanmar border:

India shares a 1643 km long border with Myanmar. Myanmar has common land with Arunachal Pradesh, Nagaland, Manipur and Mizoram. Deployment of border guarding force: Assam Rifles has been deployed for counter-insurgency and border to guard this border. Currently, all 15 border guarding battalions are deployed along Indo Myanmar border on Company Operating Base (COB) approach, not as per the BOP system. The companies are deployed on all routes of entrance/outlet and are checking infiltration, smuggling of arms, ammunition, drugs, and fake currency notes.

Management of Indo Sri Lanka and Maldives border:

India's engagement with Sri Lanka and Maldives has need for cooperation to address traditional strategic and non-traditional aspects of security in the Indian Ocean Region. The formation of the South Asian Association for Regional Cooperation (SAARC) in the 1980s had given drive and direction to regional and sub-regional cooperation despite its failure to accomplish expected objectives of regional economic and security integration in South Asia. The implementation of trilateral cooperation is influenced by overall consensus on the need for cooperation and also on the domestic political, economic and security situation within these countries. Even though Sri Lanka and Maldives have identified the convergence of interests in maritime security, competition is bound to exist. Successful implementation of the maritime security agreement will depend upon internal political and economic situation to a great extent. The fishermen issue between India and Sri Lanka is a sensitive issue involving minority communities on both sides.

Border area development programme:

The Department of Border Management, Ministry of Home Affairs has been executing a Border Area Development Programme (BADP) through the State Governments as a part of a comprehensive approach to Border Management with the aim to fulfil the special developmental needs of the people living in isolated and unreachable areas situated near the international border and to saturate the border areas with the entire essential infrastructure through convergence of Central/State/BADP/Local schemes and participatory approach and to develop security and wellbeing among the border populace.

Issues for better Border Management:

One of the important problem in managing the borders is their limitation and demarcation on the ground. India has an undemarcated border with China, Pakistan and Bangladesh. The problem of the undemarcated border is more severe with respect to Pakistan and China (Indian Defence Review, 2010). In other words, the boundaries are a mix of well recognized demarcations; International Border, LOC, LAC, Working Boundary, AGPL, McMohan Line, Disputed border. Another issue for border management is Density of population in the border areas. In some places, there is approximately 700-800 persons per sq km on the Indian side and about 1000 persons on the Pakistan side. Such an overpopulated area with a porous border poses problems in detection and apprehension of offenders who have the option of crossing over to the other side to avoid arrest. Since many villages are located so near the border there are approximately 187 villages in Kashmir where houses are located within 150 yards of International Border where the density of the population is far more than the rest of the country (Jamwal, 2002). Border Fencing raise another concern for border management. The prime aim of fencing along the Indo- Pakistan border was to check the access of criminals, stop smuggling and give security to the border population. There are wide gaps as fencing is not complete. This is due to slow progress in acquisition of land, resistance by locals, flaws in considering the project and lack of sincerity. The fencing however, has not resulted in controlling the threat to significant degree. By itself, the fencing is not a barricade. It can be operative only when it is robustly watched and kept under surveillance round the clock. The terrain, climatic conditions, dense vegetation, improper design and alignment without taking into consideration the traditions and culture of the border population, has further led to its repeated breaching. The BSF, deployed to guard the border, is stretched too thin along the border, resulting in large unmanned, unguarded gaps, which are exploited by the offenders. High snowfalls results in large stretches being waterlogged, dense vegetation and undergrowth immediately after the winters. This has severely affected the fencing which got rusted and damaged within a few years of fits commissioning. Furthermore, there are many villages between fencing and the International Boundary, where people are in conspiracy with the criminals, making detection of illegal migrants and criminal difficulties. Trouble in Identifying Foreign National is another order management issue. It is well established that Indians of the bordering States and neighbouring countries have resemblance in many ways. They look alike, speak the same language, wear the same dresses and have similar set of culture and traditions, thus it is difficult to identify a foreign national in the absence of identify cards in the border areas. Connivance of the locals with intruders for a payment makes the task of detection more difficult. Similarly at Indo - Nepal border not only the Indian and Nepalese nationals cross the

porous border without any restriction, but these days some Pakistani, Bangladeshi, Sri Lankan and even Afghan and Iranian nationals penetrate into Indian territory, misusing the open border to some extent. Their similar face, attire, posture and behaviour resemble the Napalese and Indian nationals.
Every inhabitant in India has been guaranteed the freedoms mentioned in the Preamble of our Constitution, they have to be consistent with the unity and integrity of India. Though there are numerous challenges for border management, central government is doing at its best to guard inhabitants of India. Preferably, border management should be the responsibility of the Ministry of Home Affairs during cease-fire. However, the active nature of the LoC and the need to maintain troops close to the LAC in a state of readiness for operations in high altitude areas, have forced the army to permanently deploy large forces for this task. While the BSF should be responsible for all settled borders, the responsibility for unsettled and disputed borders, such as the Line of Control (LoC) in J&K and the Line of Actual Control (LAC) on the Indo-Tibetan border, should be that of the Indian Army. The principle of 'single point control' must be followed if the borders are to be successfully managed. Despite sharing the responsibility with several para-military and police forces, the army's commitment for border management amounts to six divisions along the LAC, the LoC and the AGPL (Actual Ground Position Line along the Saltoro Ridgeline west of Siachen Glacier) in J&K and five divisions along the LAC and the Myanmar border in the eastern sector. It has been emphasized by security specialists that there should be appropriate border guidelines framed for the border guarding forces of all the nations. The aim of these border guidelines was to ensure co-operation between both the border guarding forces over cross border crimes and exchange of information and intelligence at appropriate levels. These guidelines offer that neither side to have any permanent or temporary border security forces within 150 yards on either side of International Border, and no defensive works of any nature including trenches in the stretch of 150 yards on each side of the boundary. Under this provision, Pakistan objects to the construction of fences within 150 yards from the International Border on the pretext that fencing violates the guidelines (Anand Kumar, 2010). It even objects to construction of roads within this distance on the same pretext.
This is a massive commitment that is expensive in terms of manpower as well as funds, as the deployment areas are mostly in high altitude territory, and needs to be reduced slowly. The real payoff of a reconciliation with the Chinese would be the possibility of reducing the army's deployment on the LAC. To some extent, the developments in surveillance technology, particularly satellite and aerial imagery, can support to maintain a continuous vigil along the LAC and make it possible to reduce physical deployment as and when modern surveillance assets can be provided on a regular basis to the formations deployed forward. Also, the availability of a

large number of helicopter units will improve the quality of mid-air surveillance and the ability to move troops to quickly occupy defensive positions when it becomes necessary. However, these are both pricey ventures and need to be observed in the overall context of the availability of funds for renewal. India's border security problems are many such as the penetration of armed mercenary terrorists from Pakistan, mass migrations from Bangladesh into lower Assam, the smuggling of consumer goods and fake Indian currency from Nepal, the operations of ULFA militants from safe hideouts in Bhutan and the sanctuaries available to the rebellious groups of the north-eastern states in Myanmar and Bangladesh. The nomination of the CRPF as the national level counter-insurgency force should enable the other CPMFs like BSF and ITBP to return to their prime role of better border management. To summarize, the management of India's international border along its North Eastern States has remained a critical and complex issue. In period of growing interdependence, threats from eccentric sources pose challenge to the country's security. Due to the tendency of India's neighbours to exploit the country's nation-building problems, India's internal security challenges are indistinguishably related with border management. Indian rebellious groups have for long been provided shelter across the nation's borders by hostile neighbours.

9. LINKAGES OF ORGANISED CRIME WITH TERRORISM

Organized crime mainly exploits legitimate activities for criminal purposes. The UNODC tried to give a definition to "organised crime" in the organised crime convention. So an organised crime may be defined as A group of three or more persons that was not randomly formed;Existing for a period of time;Acting in concert with the aim of committing at least one crime punishable by at least four years' incarceration; In order to obtain, directly or indirectly, a financial or other material benefit. Globalized world, lenient emigration policies, cheaper and faster international travel, social networking sites and high tech communication equipment and sophisticated money laundering methods have increased organized crimes across the world. Such gangs are engaged in anti-social activities as the use of violence and extortion, illicit drug trafficking, money laundering, acts of corruption, environmental crime, trafficking in women and children, illicit manufacturing of and trafficking in firearms, credit card fraud, computer related crime, maritime piracy, illegal trafficking of stolen vehicles, industrial espionage and sabotage etc.

Linkages of Organised Crime with Terrorism

Crime and terrorism are critical issues for security officials and investigators all around the world. Earlier, the problems of organized crime and terrorism were considered as separate phenomena but after horrified incident of September 11th attacks, researchers have started linking these two as terrorized occurrence (Shelley et al., 2015). Numerous security studies, military and law enforcement seminars thoroughly debated the evolving threat of transnational organized crime or terrorism, but the important links between the two were hardly made. It was due to the fact that organized crime and terrorism are typically viewed as two different forms of crime because the main objective of organized crime is to gain economic profit while terrorism is an act that is motivated by ideological aims and a desire for political change (Bovenkerk and Chakra, 2015).

After the Cold War and the consequent decline in state sponsorship for terrorism, the use and imitation of organized crime approaches has been an important factor as methods to generate profits for terrorist groups and equally, organized crime has adopted terrorist methods of violence. Organized crime is generally focused mainly on economic profit, acquiring material benefits and obtaining as much of an illegal

market share as possible, by the use of severe wrongdoings such as Drug trafficking, fraud, violence etc. (Baylis and Smith, 2001). Whilst terrorism motivated primarily by ideological purposes and by a desire for political change, by the use of violence, in the form of hijacking, bombing and other criminal acts.

Organised crime: Organized crime is described as any group having a corporate structure whose main aim is to obtain money through unlawful activities often surviving on fear and corruption. Today, organized crime is business at large scale that is conducting global commerce for the trafficking of illegal services and products as well as developing the associated supply chains. Criminal organizations are conducting commerce across traditional nation-state boundaries that permit illegal groups to work in synchronisation with other like groups. This coordination is called transnational crime. According to The FBI, "organized crime as any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities" (FBI 2006). These crimes include: Bribery, Murder, Counterfeiting, Embezzlement of Union Funds, Mail Fraud, Wire Fraud, Money Laundering, Obstruction of Justice, Murder for Hire Drug Trafficking, Prostitution Sexual Exploitation of Children, Alien Smuggling, Trafficking in Counterfeit Goods, Kidnapping Gambling, Arson Robbery, Sports Bribery Extortion, Drugs, and Theft from Interstate Shipment/Interstate. Organized crime is based on several factors ((Bailey and Godson 2000, Pp: 599):

1. The number of participants perceived scale of illicit operations;
2. The level of business development and organizations attributed to the social agents who live off of the illegal business or who at some point participate in that business;
3. The danger these participants may pose in specific situation for the existence or effective exercise of the rule of law.

Organized crime is intimidating global economies due to the emergence of progressive technology, growing businesses, and political pressures that generated new avenues for these criminal organizations to flourish. Organized crime involves a continuing enterprise operating for the production and sale of illegal goods and services (Jones, 2015). Organised crime has been thoroughly studied in USA since several decades. The U.S Task Force Report, 1967, appropriately describes the organised crime as "a society that seeks to operate outside the control of the American people and their government. It involves thousands of criminals working within structures as complex as those of any large corporation, subject to laws more tightly enforced than those of legitimate governments. Its actions are not impulsive but rather the result of intricate conspiracies, carried on over many years and aimed

at gaining control over whole fields of activity in order to amass huge profits". Organised crime is the joint result of the commitment, knowledge and actions of three components:

1. The Criminal groups
2. The Protectors
3. The Specialist support

The criminal group operates beyond the life time of individual members and is structured to survive changes in lead ship. The criminal group depends on continuing criminal activity to generate income. Thus, continuing criminal scheme is intrinsic in organized crime. Some activities are such as supplying illegal goods and services.

Organized crime in India is stratified, organized and administered as any other corporate office in legal business world (Gandhirajan, 2004). In India, organized crime is committed to seeking protection money, contract killing, boot-legging, gambling, prostitution and smuggling, and drug trafficking, illicit arms trading, money laundering, transporting illegitimate activities based essentially on its readiness to use physical force and violence. By corrupting public officials and thereby monopolising or near monopolising, organised crime aims to secure for itself power. Later, the money and power it creates are used to infiltrate legitimate business and several other related activities. Organised crime has been committed in India since earlier time in some form or another. It has, however, assumed its dangerous form in modern times due to several socio-economic and political factors and progressions in science and technology. Even though rural India is not resistant from it, it is essentially an urban phenomenon. In India, there is no broad law to control organised crime in all its dimensions and manifestations. There is substantive law regarding criminal scheme. According to reports, many criminal gangs of organized crimes are operating in India. These criminal gangs have been operating in India since ancient times. The gangs of 'thugs' usually preyed on travellers or wayfarers while traversing lonely regions that passed through thick jungles. The 'thugs' travelled in gangs, large or small, usually un-armed and appearing to be pilgrims, ascetics or other harmless wayfarers.

Dawood Gang: Dawood is the most dominant, Bombay gangsters having a country wide networks with linkages overseas. He is one of the most powerful gangsters involved in transnational crimes mainly narcotic drugs, smuggling, extortion and contract killing. He is operating from Dubai and some other countries since 1985. He had a phenomenal rise in short time.

Arun Gawli Gang: His gang is involved in the collection of protection money from rich businessmen and contract killings.

Other gangs are gmar Naik Gang, Chota Rajan Gang, Veerappan Gang of Karnataka, Om Prakash Srivastava or Babloo, Gang of Uttar Pradesh, Latif Gang of Ahmedabad, Rashid Gang of Calcutta.

Terrorism: Terrorism is an act that appears to be intended to terrorise or force a civilian population to influence policy of a government by extortion or to affect the conduct of the government by assassination or abduction. Theoretical studies have documented that Terrorism usually results from multiple causal factors - not only psychological but also economic, political, religious, and sociological factors, among others. There is even a hypothesis that it is caused by physiological factors. Because terrorism is a multi-causal phenomenon, it would be simplistic and erroneous to explain an act of terrorism by a single cause, such as the psychological need of the terrorist to perpetrate an act of violence (Hudson 1999, 15). It is established in theoretical studies that terrorists are not a consistent group but their roots are diverse.

Terrorism counteracts the most basic values of cultivation. Previous literatures have shown that terrorism is practiced since ancient time and executed in various forms. During 20th century, the occurrence of terrorism was focused on bully or their representatives. Terrorism is evolved as new perilous missile to undermine the government activities and disrupt important services. When reviewing literature, various intellectuals and security professionals elaborated the concept of terrorism. According to The U.S. Department of State (DOS), terrorism as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience (U.S. DOS 2003). The Federal Bureau of Investigation described the occurrence of terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce Government, the civilian population, or any segment thereof, in furtherance of political or social objectives (Jarboe 2002).

The Department of Defense (DOD) delineates the calculated use, or threatened use, of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives (FM 1-02 2004, 1-186). The UN described terrorism as criminal and unjustifiable, wherever and by whomsoever committed; terrorism are criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance

unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them (UNODC 2006c). The objective of terrorist organizations is different from the ideology they embrace and the country they are active in. General purpose of terrorism seems like to overthrow its target regime and to establish a new system in the light of their ideology. (Dilmaç 2006, 451)

Some causal factors impact contrarily on various types of terrorist groups. Many researches designated that technical advancement significantly affects the level of ideological terrorism in any country. In some cases, terrorist groups attack due to one set of causes and continually active for over a period of time for different reasons. In many cases, terrorism emerged due to conflicts among groups. Some reports demonstrate some groups involve in terrorism because they have tried other alternatives. Other groups adhere to terrorist because they have learned from the experiences of others, usually through the news media. Terrorist organizations such as Osama bin Laden and his al Qaeda organization developed that is fundamentally different from previous type terrorist groups to target innocent public. With lethal attack of the September 11 Bin Laden accomplished his political objective.

There are numerous types of terrorism:

1. **State Terrorism:** It is an act committed by government. Many researchers consider that the actions of governments can be labelled terrorism such as using the term 'terrorism' to mean violent action used with the predominant intention of causing terror. It has been said that State terrorism" is as contentious concept as that of terrorism itself. Terrorism is often, describe four characteristics that include the threat or use of violence, a political objective, the desire to change the status quo, the intention to spread fear by committing spectacular public acts, and the intentional targeting of civilians.
2. **International Terrorism:** These are identified as acts planned, executed across more than one nation. International terrorism is the illegal use of force or violence committed by a group or individual, who has some connection to a foreign power or whose activities transcend national boundaries, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
3. **Domestic Terrorism:** Acts planned, executed in one nation. Domestic terrorism involves groups or individuals who are based and operate entirely within nation like the United States and Puerto Rico without foreign direction and whose acts are directed at elements of the U.S. Government or population.

The arsenals that domestic terrorist groups have access to and have stockpiled in caches around their areas of operation are difficult. Extremists have amassed explosives, machine guns, missiles and other weapons. These groups are also trained by experienced war veterans, police officers, "guns for hire," ex-special forces members, demolitions experts, and other highly skilled survivalist that train them in the art and science of war.

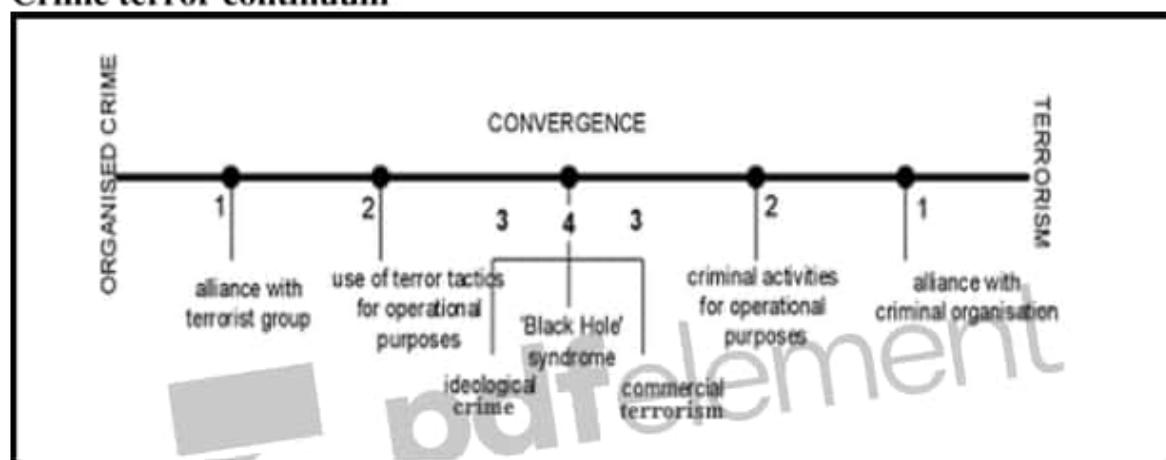
4. **Religious Terrorism:** Religious terrorism is a type of terror activity that is done on motivations and goals that have a mainly religious character or influence. In contemporary situation, after the decline of concepts such as the heavenly right of kings and emergence of nationalism, terrorism has more often been based on anarchism, nihilism, and revolutionary politics. Since 1980, however, there has been an upsurge in terrorist activity motivated by religion. Reports of the Global Terrorism Index have shown that since 2001, religious extremism has overtaken national separatism to become the main driver of terrorist attacks around the world.

Modern literature relates to terrorism in the context of religion and its Diasporas. This is not surprising given the events that have dominated global attention since over a decade. In addition to Islamic terrorist groups, the Tri-Border Area (TBA) provides a haven that is geographically, socially, economically, and politically highly conducive for allowing organized crime and the corrupt officials who accept their bribes or payoffs to operate in a symbiotic relationship that thrives on drug and arms trafficking, money laundering, and other profitable criminal actions. It can be established that Terrorism is a global phenomenon and in 2013 attacks were carried out in 87 countries with 60 of these experiencing deaths from terrorism.

Reports indicated that terrorism is increased by 70 per cent in India from 2012 to 2013, with the number of deaths increasing from 238 to 404. The number of attacks also increased, with 55 more attacks in 2013 than 2012. However, the majority of terrorist attacks in India have low casualties. In 2013, approximately, 70 per cent of attacks were non-lethal. There were attacks by 43 different terrorist groups such as Islamists; separatists; and communists. Communist terrorist groups are by distant the most frequent perpetrators and the main cause of deaths in India. Usually, the difference with Pakistan over Jammu and Kashmir is main cause of Islamic terrorism. In 2013 three Islamist groups were responsible for around 15 per cent of deaths. This includes Hizbul Mujahideen, an Islamist group allegedly based in Pakistan with a membership of around 15,000. This group was the only group in India to use suicide tactics in 2013. North east region of India has for the last three decades seen continual ethno-political unrest from ethnic secessionist movements. Separatist groups including in Assam, Bodoland, Kamtapur and Meghalaya were responsible for 16 per cent of deaths.

Previously, inspirations for terrorism and organized crime were different. The main intent of terrorism was to chase power; gaining of power and to use power through political, ideological, religious or ethnic means but organized crime was for money and power through illegal movement.

In present global condition, most terrorists are involved in some form of organized crime and a rising number of organized crime lobbies are engaging in political violence. While some terrorist organizations may only profit briefly or indirectly from organized crime, others unite and become a hybrid organization displaying both characteristics.

Similarity in the features of organised crime and terrorism:

1. Both have hierarchical structure.
2. In both act, there is limited membership.
3. In both criminal act, there is a violence to achieve goals.
4. There are Rules and regulations that define behaviour.

Linkages of Organised Crime with Terrorism:

In present global climate, high profile crime is committed to gain power and generate huge funds to live lavishly. Researchers have stated that there is strong link between terrorists with criminal organizations. Primarily, crime and terrorism are slightly related in meaning and strategic application; however, historically these organizations have differing motivations, and ideologies. Crime is usually

encouraged by financial gain, while terrorism has been primarily motivated by philosophy such as Maoism, Marxism, or theological ideologies. According to John R. Wagley, "terrorists are increasingly seen as supporting themselves through criminal activity, because a growing number of extremists may feel justified in committing the criminal activities themselves, on the grounds that such acts square with their ultimate terrorist aims" (Wagley 2006). In an example of funding for the March 2003 Madrid train attacks came from drug dealing and the Dubai-based Indian mobster, Aftab Ansari, is believed to have helped fund the September 11 attacks with ransom money earned from kidnapping" (Wagley 2006, 3).

Crime terror continuum

Criminals see other benefit from linkage of organized crime and terrorists activities is that this relationship is established techniques, tactics, and procedures (TTP) against law implementation, the government, and social institutions in a particular nation. These techniques, tactics, and procedures are vital as criminals can teach terrorists the weaknesses of the country's rule of law, how to operate without recognition under the radar, the least detectable communication methods such as cell phone burners, Morse code, child messengers, encrypted websites like Hushmail, or letters with simple encryption and how to use already well-developed criminal supplies such as arms dealers, the narcotics trade, and money laundering services.

The occurrence of globalization and dreaded incident of the 9/11 on the World Trade Center have made the conditions to link between organized crime and terrorism to grow at huge scale. This trend is rising due to the U.S. governmental crackdown on rebellious funding in which "153 individuals, organizations, and financial supporters of terrorism" access to financial networks were severely reduced or eliminated by the 29-nation Financial Action Task Force (Bush 2001, paragraph 24-31). Other reasons are the need to create revenue, the use of well-developed criminal supply

chains and networks, and the interdependent relationship that criminals and terrorists share.

In general, there appear to be three ways that the crime-terror nexus interact:

1. Through shared tactics and methods;
2. Through the process of transformation from one type of group to the other over time; and JMLC
3. Through short- or long-term transaction-based service-for-hire activities between groups (Mullins, 2009).

There are many similarities between terrorist organizations and organized crime groups. Uyar, (2006) describe these stands as following:

1. First similarity is that both operate secretly. Although both terrorist groups and criminal organizations have a strong central leadership, they are mainly based on cell structures to achieve their own goals. Day to day operations are carried out by members of small cells.
2. Both use violence and produce mostly civilian victims.
3. Intimidation and fear are characteristics of both groups.
4. They use similar tactics, such as kidnapping, assassination, extortion.
5. Terrorist and crime group organizations use front organizations such as legitimate businesses or charities.
6. Both uses similar ways to conceal profits and fund raising.
7. The activities of both groups are in cross the national-regional transnational divide; both groups require safe havens, and as a result both tend to take advantage of Diaspora communities.
8. Both groups are aided by corrupt officials whose services provide mutual benefits, such as access to fraudulent documents, including passports and other identification and customs documents to smuggle goods and weapons.

It can be said that both terrorism and organized crime use of similar methods without working together. Each group relies upon support and expertise of others. There is a symbiotic relationship in both acts. Groups develop cooperative relationship to defend each other. As described earlier in this paper. The FBI definition of organized crime does not relate to the many of description of terrorism; however, the activities of organized crime match-up with the acts of terrorism, in that terrorism uses fierce acts to attain a particular goal. It is well understood in various reports that Crime and terrorism have occurred under various conditions and are multi-causal occurrence.

Theories of Anomie, Repressive Regime, Conflict, and Differential Opportunity. Elaborated the elements of the crime and terrorism phenomenon.

There is huge supportive literature that shows the linkage between organized crime and terrorism. Both crime and terrorism have occurred under parallel conditions. These conditions comprise of economic adversity, social stratification, oppressive regimes, weak or limited law enforcement, socioeconomics, and the politics of a particular region. Both crime and terrorism allow the marginalised or the subjugated to gain life success by choosing another path that breaks the institutional barriers of entry using innovative, illegal approaches. These methods provide opportunities for ideological wins, financial advantage and vertical movement in a society. Subsequently, the socio-political and socioeconomic environment can actually empower criminal and terrorist elements. Other factors like high joblessness, poverty, the lack of education, the lack of opportunities, high infant mortality rates, and cultural/religious relations; all contribute to criminal and terrorist trends.

According to Uyar (2006), terrorist organizations are distinguished from organized crime groups on the basis of following features:

1. Terrorist organizations are normally ideologically, politically, or religiously motivated while organized crime groups are profit oriented. Dissimilar to this fact, terrorist groups that usually have non-financial goals: publicity, dissemination of an ideology, the destruction of a society or regime, and simply spreading terror and intimidation, drug traffickers and organized crime groups first and foremost seek monetary gain.
2. Terrorist groups often wish to contest with governments for legitimacy, but organized crime organizations do not.
3. While terrorist organizations usually enjoy media attention, organized groups do not.
4. Generally, terrorist victimization is less discriminate than the violence used by organized crime groups.

Nexus between organized crime and terrorism increases also due to many factors such as globalization in which free flow of trade and human provide opportunity for both to intermingle, communication rebellion through internet, end of cold war that reduce state financing of terrorist therefore terrorist indulge in criminal activities to fill financial needs and lastly, global war on terror. Terrorism and organized crime shared techniques. Internet and cyberspace are crucial tools for recruitment, propaganda, planning, logistics, fund raising, and money laundering.

Linkages of organised crime with terrorism in India:

In Northeast, numbers of insurgent groups over a time have morphed into crime syndicates. All militant group run a similar government or have their areas of influence involved in collecting money directly from people, and from government funds due to misgovernance, government officials are threatened or bribed to award contracts and also important commodities like rice and kerosene are sold to public at much higher rate. There are growing number of extortion, kidnap, contracts, black marketing transnational drugs and arms to finance terrorism. In India, there is infamous entry points from Southeast Asia to India- moreh and Chittagong hill tract especially coxs bazaar. When discussing about Kashmir, unlike northeast reliance of funds from extortion and other related means is minimal. External funds by Pakistan and other countries especially gulf.

Other linkage is through the spread of fake currency. Terrorists are the main agent of this currency. Indian mujahidin resorted to crime to raise funds. This includes robberies and kidnapping. Maoists terror movement also uses coercion, robberies of banks and kidnapping to collect huge funds.

To summarize, Union of organized crime and terrorism is major menace for international safety and peace. These crimes are growing at rapid rate. It can be concluded from reviewing major facts of these crimes that Organized crime is a rising as international phenomenon and, as it intersects with terrorism, an increasingly dangerous force. Although terrorism and organized crime are dissimilar horrified criminal activities, the important fact is that terrorists and criminal networks overlay and collaborate in some situation. Regrettably, the interaction of terrorism and organized crime is increasing because of parallel conditions give rise to both and because terrorists and organized criminals use similar approaches to promote their operations. Unfortunately, their alteration of incorporating fraud into their larger criminal goals is deadly. Just as terrorists pool their abilities and resources to achieve synergistic outcomes. Its abolition can be possible only if collaboration is attained at global scale and counter-terrorism programs along with development schemes are executed at fundamental level.

10. MONEY LAUNDERING AND TERRORISM FINANCING

Over the decades, India (as well as other parts of world) has witnessed numerous terror strikes and still remains a potential target for terror related activities. These attacks certainly cannot be carried out without the help of money. Financing is needed not just to fund specific terrorist operations, but also to meet the broader organizational costs of developing and maintaining a terror organization and to create an enabling environment necessary to sustain its activities. FATF (Financial Action Task Force) highlights several requirements of terror organisations for which they require funding –

- The direct costs of terrorist attacks like procuring precursor materials necessary to stage specific attacks like vehicles, improvised bomb-making components, maps, surveillance material etc.
- Salaries / subsistence for its operatives and their dependent family members
- Recruitment & Training of operatives in terms of both ideological indoctrination and practical skills.
- Some terror groups also sustain Charitable organisations and Businesses to give their organisation a masquerade of legitimacy. Such organisations and businesses not just require funding but at times can also act as a source of funds for terror organisations.
- For terror organizations, often a sophisticated public relations and media operations component that sustains the ideology of terrorism requires significant funding. For example - the propaganda over the internet by ISIS to spread its ideology and increase the number of recruits.

Therefore, uprooting terror finance networks/channels creates a hostile environment for terrorism, constraining overall capabilities of terrorists and frustrating their ability to execute attacks.

The Role of Money Laundering

Since terror activities cannot be financed from legal sources of money, Money Laundering serves as an important mode of terrorism financing. Terrorists have shown adaptability and opportunism in meeting their funding requirements. Terrorist organizations raise funding from diverse sources, including the abuse of

charitable entities or legitimate businesses or self-financing by the terrorists themselves. It is here that the nexus between terrorism and money laundering is evident –

- Exploitation of Charities - Charities or non-profit organisations possess characteristics that make them particularly attractive to terrorists or vulnerable to misuse for terrorist financing. They enjoy the public trust, have access to considerable sources of funds, and their activities are often cash-intensive. Furthermore, some charities have a global presence that provides a framework for national and international operations and financial transactions, often in or near areas most exposed to terrorist activity. Finally, charities are subject to significantly lighter regulatory requirements than financial institutions or publicly held corporate entities. Therefore, proceeds from such charitable institutions are often laundered to fund terror activities.
- Diversion from legitimate Businesses – Often terror organisations run legitimate businesses and profits/proceeds from such businesses are laundered to fund terror activities. Particular in these are cash intensive businesses like gambling houses/casinos etc. and businesses where it is difficult to keep a track of sales/services being offered.
- Criminal Activities - Terrorist use of criminal activity to raise funds ranges from low-level fraud to involvement in serious and organised crime such as arms trafficking, kidnap-for-ransom, extortion, racketeering etc.
- Drug Trafficking - Drug Trafficking is an attractive source of funds for terrorist groups, enabling them to raise large sums of money. For ex- Al Qaeda's one of the largest sources of fund is sale of Opium. Similarly, several terror outfits operating in East/South-east Asia utilize funds from trafficking of Cocaine from Golden Triangle. Investigations and intelligence have revealed direct links between various terrorist and drug trafficking organisations that frequently work together out of necessity or convenience and mutual benefit.
- Credit Card Fraud - There is a market for illegally obtained personal details, including credit card account numbers, as well as personal information such as the card holder's full name, billing address, telephone number, start and expiry dates, the security number on the rear of the card, etc. This remains one of the most exploited markets for terror organisations.
- Cheque Book Fraud - Several cases have been identified in which a basic model of bank fraud has been applied to generate funds for terrorism. These cases involved bank accounts being opened using false identity documents and fraudulent deposits. Cheque books are then stockpiled; and when a large number have been accumulated, they are used to purchase goods from

department stores costing under the amount that would trigger verification to ensure sufficient funds were available in the account. The goods are returned for a cash refund.

- Trade - Trade of merchandise and natural resources (like ISIS controlling Petroleum fields) are other sources of terror financing. As international trade today has grown several folds, thereby providing terrorist organisations the opportunity to transfer value and goods through seemingly legitimate trade flows. The proceeds from such activities are laundered off to terror organisations.

(As per a latest report by FATF, trade accounts of diamond business in India are being used to launder illegal funds and finance terror activities. As there are no set standards of diamond pricing in the country, agents are overvaluing the costly and prized gemstones for purposes of laundering and suspected financing.)

International Response

As per FATF, terrorist organisations' diverse requirement for financing creates a strong logic for seeking to disrupt terrorism by choking off funding flows to all terrorist-linked activities. Interdicting these flows can degrade the capability of terrorist groups over time, limiting their ability to launch attacks, increasing their operational costs and injecting risk and uncertainty into their operations, which can have tactical benefits, such as damaging morale, leadership and legitimacy within a network. Therefore, the steps that should or are being taken are –

- Preventing Terrorists from Raising, Moving, and Using Funds – Detecting terrorist involvement in otherwise legitimate financial activity requires financial institutions to implement the FATF standards through strong application of the KYC – (know your customer) principle and of customer due diligence (CDD) policies and procedures. These are also fundamental to the reporting of suspicious transactions that may indicate criminal activity supporting terrorism. To assist financial institutions in combating terrorist financing, jurisdictions must adopt certain measures. These include implementing targeted financial sanctions programmes, protecting vulnerable sectors including the charitable sector and money-service businesses, and encouraging effective reporting of suspicious activity.

- Targeted Financial Sanctions - FATF calls on countries to develop and implement targeted financial sanctions regimes that identify, freeze the assets

of, and prohibit making funds available to designated terrorists and their support networks.

- Protecting Vulnerable Sectors - FATF lays out a framework that aims to protect the non-profit organisations/NGOs/charitable sector by ensuring it is not misused by terrorist organisations. The framework includes, supervision and monitoring of such institutions and international agreements to control their misuse.
- Suspicious Transaction Reporting - Financial information including that gathered from suspicious transaction reporting has a central role in identifying terrorist financing and the movement of terrorist funds through the financial system. Financial information alone may not be sufficient to identify terrorist financing activity. However, when combined with counter-terrorist intelligence drawn from surveillance of the range of terrorist activities and networks, financial information can be leveraged to provide financial institutions with a concrete indication of possible terrorist activity.
- Financial information - Through the development of internationally recognised AML and CFT (Anti Money Laundering and Combating Financing of Terror) standards, financial institutions and other designated non-financial entities have taken steps to know their customers and keep records.

India's Response

India became FATF's 34th Member in June 2010. As per the FATF procedure, every country has to give an Action Plan to bring their AML/CFT regime close to the compliance zone of the FATF. India also gave an Action Plan in June 2010 and followed up with Action Taken Report in October 2010 and in February 2011.

- In line with the FATF standards, RBI has introduced strict KYC norms for Banking related activities. On its part SEBI has also tweaked its KYC norms for market related transactions.
- The Unlawful Activities (Prevention) Act, 1967(UAPA) and the Prevention of Money laundering Act, 2002 (PMLA) are effective instrumentalities to combat offences relating to Terrorist Financing and Money laundering. The Unlawful Activities (Prevention) Act, 1967 has been strengthened by amendments in 2013 which inter-alia includes enlarging the scope of proceeds of terrorism to include any property intended to be used for terrorism
- A special Combating Financing of Terrorism (CFT) Cell has been created in the Ministry of Home Affairs in 2011, to coordinate with the Central

Intelligence/Enforcement Agencies and the State Law Enforcement Agencies for an integrated approach to tackle the problem of terror funding.

- Also, a Terror Funding and Fake Currency Cell has been set up in the National Investigation Agency to investigate Terror Funding cases.
- Moving with FATF standards, FIU (Financial Intelligence Unit) India has been established to monitor suspicious financial transactions that could be related to terror finacing.
- SEBI is intensively cracking down on Shell Companies that could be involved in money laundering or generating resources for terror financing.
- For past several years, the government is cancelling the registration of NGOs which are not filing timely returns/reports under FCRA or Foreign Currency Regulation Act.
- Finally, the Narcotics Act of India is being implemented to curb the menace of drug trafficking. Also, the BSF and other border security agencies are keeping a special check on cash couriers and drug mules as often these are related to terror financing.
- India has reformed its AML/CFT standards as per standards set by FATF as well as Asia Pacific Group. ***In addition, recently India entered into an agreement with UAE to curb Money Laundering and Terror Financing.***

What more could be done

- Jurisdictional Issues - There are concerns about the terrorist financing vulnerabilities associated with safe havens, failed states or state sponsors that create enabling environments or otherwise provide active support to terrorist organisations. Through international cooperation these issues need to be resolved.
- Enhanced Financial Intelligence - Financial information alone is not sufficient to effectively combat terrorism. However, when combined with counter-terrorist intelligence, financial information can greatly enhance a country's ability to identify and intercept terrorist activity.
- Outreach to the private sector for implementing FATF guidelines effectively in close cooperation with the state agencies.
- Creating a better understanding of link between Money Laundering and Terror financing at the levels of state, institutions (public/private) and individuals

11.SECURITY FORCES, SECURITY ORGANISATIONS AND THEIR MANDATES

INDIAN ARMED FORCES

- The Indian Armed Forces are the military forces of the Republic of India. It consists of three professional uniformed services: the Indian Army, Indian Navy, Indian Air Force.They have HQ at Delhi.
- The President of India is the Supreme Commander of the Indian Armed Forces. The Indian Armed Forces are under the management of the Ministry of Defence (MoD), which is led by the Union Cabinet Minister of Defence.
- Additionally, the Indian Armed Forces are supported by three paramilitary organisations (Assam Rifles, Indian Coast Guard and Special Frontier Force) and various inter-service institutions such as the Strategic Forces Command.

Indian Army

- Motto: "Service Before Self"
- The Indian Army originated from the armies of the East India Company, which eventually became the British Indian Army and finally the national army after independence.
- It has third largest active military personnel in the world.
- It is the land-based branch and the largest component of the Indian Armed Forces. The President of India serves as Commander-in-Chief of the army, and it is commanded by the Chief of Army Staff (COAS).
- The Indian Army is operationally and geographically divided into seven commands, with the basic field formation being a division. It has 34 Divisions.
- It is divided into six operational commands (field armies) and one training command.
- Ghatak Commandos is a special operations capable infantry platoon.

Role and Mandate of Indian Army

- The primary mission of the Indian Army is to ensure national security and unity, defending the nation from external aggression and threats, and maintaining peace and security within its borders.

- It conducts humanitarian rescue operations during natural calamities and other disturbances, like Operation Surya Hope (response in Uttarakhand following the June 2013 North India floods), Operation Megh Rahat (Jammu Kashmir Flood in 2014).
- It can also be requisitioned by the government to cope with internal threats.
- The army has been involved in four wars with neighbouring Pakistan and one with China. Other major operations undertaken by the army include Operation Vijay (Kargil War 1999), Operation Meghdoot (to capture the Siachen Glacier in the Kashmir region in 1984), Operation Cactus (to foil 1988 Maldives coup d'état attempt by a group of Maldivians led by Abdullah Luthufi and assisted by armed mercenaries of a Tamil secessionist organisation from Sri Lanka).
- Apart from conflicts, the army has conducted large peace time exercises like Operation Brasstacks and Exercise Shoorveer.
- It has also been an active participant in numerous United Nations peacekeeping missions including the ones in Cyprus, Lebanon, Congo, Angola, Cambodia, Vietnam, Namibia, El Salvador, Liberia, Mozambique and Somalia. In 2014 India was the third largest troop contributor with 7,860 personnel deployed with ten UN Peacekeeping Missions of which 995 are police personnel, including the first Female Formed Police Unit under the UN.

Indian Air Force

- Motto:"Touch the Sky with Glory"
- Its the World's 4th largest Airforce.
- It was officially established on 8 October 1932 as an auxiliary air force of the British Empire. (Air Force Day: 8 October)
- The President of India is the Supreme Commander of all Indian armed forces and by virtue of that fact is the notional Commander-in-chief of the Air Force. Chief of the Air Staff with the rank of Air Chief Marshal is the Commander of the Indian Air Force. He is assisted by six officers, all with the rank of Air Marshal
- Command: The Indian Air Force is divided into five operational and two functional commands. Each Command is headed by an Air Officer Commanding-in-Chief with the rank of Air Marshal. Two functional commands – Maintenance Command and Training Command.
- Wing: A Wing is a formation intermediate between a Command and a Squadron. It generally consists of two or three IAF Squadrons.

- Squadron: A squadron is mainly a unit comprising a number of aircraft and their aircrews, usually of the same type. The current squadron strength of the force is 33. A squadron comprises around 18 to 20 aircraft. Target is 42 squadron.

Role and Mandate of Indian Air Force

- Its primary responsibility is to secure Indian airspace and to conduct aerial warfare during a conflict.
- Since independence, the IAF has been involved in four wars with neighbouring Pakistan and one with the People's Republic of China. Other major operations undertaken by the IAF include Operation Vijay (the annexation of Goa from Portugal), Operation Meghdoot, Operation Cactus and Operation Poomalai (to air-drop supplies over the besieged town of Jaffna in Sri Lanka on 4 June 1987 in support of Tamil Tigers during the Sri Lankan Civil War).
- It is also involved during humanitarian crisis. Operation Raahat was an operation of the Indian Armed Forces to evacuate Indian citizens and other foreign nationals from Yemen during the 2015 military intervention by Saudi Arabia.
- Apart from conflicts, the IAF has been an active participant in United Nations peacekeeping missions.

Garud Commando Force

- The Garud Commando Force is the Special Forces unit of the Indian Air Force. It was formed in September 2004.
- Garud is tasked with the protection of critical Air Force bases and installations; search and rescue during peace and hostilities and disaster relief during calamities. Presently, Garud's are deployed in Congo as part of the UN peace keeping operations.

Air Force Network (AFNET)

- The Air Force Network (AFNET), a robust digital information grid that enabled quick and accurate threat responses, was launched in 2010, helping the IAF become a truly network-centric air force. AFNET is a secure communication network linking command and control centres with offensive aircraft, sensor platforms and ground missile batteries.

Indian Navy

- Motto: शं नो वरुणः (May the Lord of the Oceans be auspicious unto us)
- The President of India serves as the Commander-in-Chief of the Navy. The Chief of Naval Staff (CNS), in the rank of Admiral, commands the navy.
- The Indian Navy has its origin in 1947.
- The Indian Navy operates three Commands. The Eastern (Vizag), Western (Mumbai) and Southern (Kochi) Commands. Each Command is headed by a Flag Officer Commanding-in-Chief of the rank of Vice Admiral.

Role and Mandate of Indian Navy

- The primary objective of the navy is to secure the nation's maritime borders, India also uses its navy to enhance its international relations through joint exercises, port visits and humanitarian missions, including disaster relief. In recent years, the Indian Navy has undergone rapid modernisation to replace its ageing equipment and developed blue-water capabilities and enhanced its position in the Indo-Pacific region.

Marine Commando Force (MCF)

- The Marine Commando Force (MCF), also known as MARCOS, is a special forces unit that was raised by the Indian Navy in 1987 for direct action, special reconnaissance, amphibious warfare and counter-terrorism.
- In 1988, the MARCOS successfully rescued several hostages, including Maldives' then-Minister of Tourism, aboard a ship hijacked by PLOTE mercenaries during Operation Cactus.
- During the 26/11 Mumbai attacks, the MARCOS were also involved in the rescue mission of hostages captured by the terrorists in Taj hotel in Mumbai in November 2008.

Integrated Space Cell

- The Integrated Space Cell is the nodal agency within the Government of India which oversees the security of its space based military and civilian hardware systems. It will be jointly operated by all the three services of the Indian Armed Forces, the civilian Department of Space and the Indian Space Research Organisation (ISRO).

- The Integrated Space Cell has been set up to utilize more effectively the country's space-based assets for military purposes and to look into threats to these assets.
- It functions under the Integrated Defense Services headquarters of the Indian Ministry of Defense.

Andaman and Nicobar Command

- The Andaman and Nicobar Command is a Tri-service theater command of the Indian Armed Forces, based at Port Blair in the Andaman and Nicobar Islands, a Union Territory of India. It was created in 2001 to safeguard India's strategic interests in Southeast Asia and the Strait of Malacca by increasing rapid deployment of military assets in the region.
- The Andaman and Nicobar Command is India's first and only joint tri-service command, with rotating three-star Commanders-in-Chief from the Army, Navy and Air Force reporting directly to the Chairman of the Chiefs of Staff Committee

Cold Start Doctrine

- Cold Start is a military doctrine developed by the Indian Armed Forces for use in a possible war with Pakistan. (it is not 'official'). The Cold Start doctrine is intended to allow India's conventional forces to perform holding attacks in order to prevent a nuclear retaliation from Pakistan in case of a conflict
- Cold start doctrine involves following:

1. Limited but precise strikes in enemy state to prevent nuclear retaliation.
2. Capture small but strategic territories in Pakistan- which can be traded for concessions later on.

PARAMILITARY FORCES

- The term "paramilitary forces" in India has not been defined in any acts or by authorities officially however they are conventionally used to refer to three forces i.e. Assam Rifles, Special Frontier Force and Indian Coast Guard. They assist Armed forces very closely and led by officers of Indian Armed forces.
- Previously term 'Paramilitary forces' was used to refer to variety of armed services that aid the operation of law enforcement agencies of India and Armed forces but in 2011 on request of army a new definition was adopted

which excluded Central Armed Police forces. From March 2011, Ministry of Home Affairs adopted a uniform nomenclature of Central Armed Police Forces for five forces namely CRPF, BSF, ITBP, CISF, SSB (which are generally led by IPS office and is under Home Ministry) to avoid confusion

Indian Coast Guard

- Motto: वयम् रक्षामः (We Shall Protect)
- Emergence of the Coast Guard in India in 1977 as a new service was the result of an awareness that had been growing for some time in the Government for the requirement to enforce National Laws in the waters under national jurisdiction and ensure safety of life and property at sea. The Indian Coast Guard was formally established on 18 August 1978 by the Coast Guard Act, 1978 of the Parliament of India as an independent Armed force of India . It operates under the Ministry of Defence.
- It protects India's maritime interests and enforces maritime law, with jurisdiction over the territorial waters of India, including its contiguous zone and exclusive economic zone.
- The Indian Coast Guard organisation is headed by the Director General who is located at Coast Guard Headquarters (CGHQ), New Delhi.
- Except Director General who is an Indian Navy officer, all others are directly appointed.
- The Coast Guard works in close cooperation with the Indian Navy, the Department of Fisheries, the Department of Revenue (Customs) and the Central and State police forces.

Role and Mandate of Indian Coastal Guard:

- Ensuring safety and protection of the artificial islands, offshore installations and other structure in our maritime zones.
- Providing protection to fishermen and assistance to them at sea while in distress.
- Preservation and protection of our maritime environment including prevention and control of maritime pollution.
- Assistance to the Department of Custom and other authorities in anti-smuggling operations.
- Enforcement of MZI Acts.
- Initiating measures for the safety of life and property at sea.
- Law enforcement in territorial as well as international waters

- Scientific data collection and support
- National defence during hostilities (under the operational control of the Indian Navy)

Additional responsibilities:

- Offshore Security Coordination Committee (OSCC) – The Director-General of the Indian Coast Guard is the chairman of OSCC constituted by the Ministry of Petroleum and Natural Gas.
- National Maritime Search and Rescue Coordinating Authority (NMSARCA) – The Director-General of the Indian Coast Guard is the NMSARCA for executing / coordinating search and rescue missions
- The Director-General of the Indian Coast Guard is the commander of coastal command and is responsible for overall coordination between central and state agencies in all matters relating to coastal security.
- Lead Intelligence Agency (LIA) – For coastal and sea borders.

Assam Rifles

- Motto: Friends of the Hill People
- HQ: Shillong
- The Assam Rifles is the oldest paramilitary force of India.The unit can trace its lineage back to a paramilitary police force that was formed under the British in 1835 called Cachar Levy. The Force was raised mainly to guard the alluvial plains of Assam from the wild and unruly tribes inhabiting the surrounding hill tracts. Since then the Assam Rifles have undergone a number of name changes before the name Assam Rifles was finally adopted in 1917 in recognition of its contribution to the war effort during World War I.
- The Force has been officered by Army Officers since 1884.
- The Assam Rifles contribution towards assimilation of the people of the North-East into the national mainstream is truly monumental. Their long association with the region reflects in the force being fondly called "The Sentinels of the North-East" and "Friends of the Hill People". During its long history, the Assam Rifles has earned many laurels both in aid to the civil administration as also fighting alongside the Army.
- It is now under Assam Rifles Act, 1941.

Role and Mandate of Assam Rifles

- Assam Rifles is under the governing control of the Indian Ministry of Home Affairs (MHA) and they perform many roles including the provision of internal security under the control of the army through the conduct of counter insurgency and border security operations, provision of aid to the civil power in times of emergency, and the provision of communications, medical assistance and education in remote areas.
- In times of war they can also be used as a combat force to secure rear areas if needed.
- A helping hand for humanitarian causes and in natural calamities.
- Undertakes development activities in the North-East by way of construction of roads and tracks, water sup schemes, schools, community halls, play grounds for village children and repair/ maintenance of buildings in the remote areas.
- Since 2002 It is Border Guarding Force for the Indo – Myanmaar border as per the government policy "one border one force" and is also its lead intelligence agency.
- It is also involved in active counter insurgency operations and law and order.

Special Frontier Force

- The Special Frontier Force (SFF) was created on 14 November 1962. Its main goal originally was to conduct covert operations behind Chinese lines in the event of another Sino-Indian War.
- The SFF came to be known as 'Establishment 22' due to its first Inspector General, Major General (Retd.) Sujan Singh Uban of Indian Army, who used to be commander of 22 Mountain Regiment during World War II.
- Based in Chakrata, Uttarakhand, the force was put under the direct supervision of the Intelligence Bureau, and later, the Research and Analysis Wing, India's external intelligence agency.
- SFF was extremely successful against Pakistan during the Indo-Pakistan Military Conflict of 1971. They trained the Bangladeshi underground unit, Mujib Bahini for their secret missions.
- SFF was used in combating communal riots in mid 1970s and later was used in Operation Blue Star in 1984. It was also used briefly for VIP security in late 1984 around the Prime Minister following the assassination of Indira Gandhi. Later this role fell upon the Special Protection Group.

- In 1975 a new rule pertaining to the SFF was issued, this prohibited the SFF from being deployed to within 10 km of the Indo-Chinese border unless under explicit instructions. This came about after several incidents in which SFF was found to be conducting unsanctioned cross-border raids and intelligence operations.
- Currently, one SFF battalion is stationed in the Siachen Glacier.

CENTRAL ARMED POLICE FORCES

- The Central Armed Police Forces (CAPF) refers to five security forces in India under the authority of Ministry of Home Affairs. They are Border Security Force, Central Reserve Police Force (CRPF), Central Industrial Security Force (CISF), Indo-Tibetan Border Police (ITBP) and Sashastra Seema Bal (SSB).
- Five CAPFs, the BSF, CRPF, ITBP, CISF & SSB, are organized on police lines. These CAPF have their own cadre of officers, but headed by officers of the Indian Police Service.
- On the recommendation of Border Management Task Force which was constituted after Kargil war, provision was made for One Border One force and accordingly various forces were created.

Border Security Force

- Motto: "Duty Unto Death". Its ethos is "Any task, any time, any where"
- Border Security Force Act, 1972
- Headquarters at New Delhi
- The Border Security Force (BSF) is the primary Border Guarding police force of India. It was raised in the wake of the 1965 War on 1 December 1965, "for ensuring the security of the borders of India and for matters connected there with". Till 1965 India's borders with Pakistan were manned by the State Armed Police Battalion.
- The BSF has its own cadre of officers but its head, designated as a Director-General (DG), since its raising has been an officer from the Indian Police Service.
- It currently stands as the world's largest border guarding force. BSF has been termed as the First Wall of Defence of Indian Territories.
- BSF is the only Central Armed Police force to have its own Air Wing, Marine Wing and artillery regiments, which support the General Duty Battalions in their operations.

- The BSF maintains a Tear Smoke Unit (TSU). The TSU is responsible for producing tear gas munitions required for the Anti-Riot Forces.
- The BSF also has a national level school for breeding and training of dogs.
- Three battalions of the BSF, located at Kolkata, Guwahati and Patna, are designated as the National Disaster Response Force (NDRF). The battalions are equipped and trained for all natural disasters including combating Nuclear, Biological and Chemical (NBC) disasters.
- Creek Crocodile Commando: In order to thwart landing of terrorists through the sea route, BSF has formed its first commando unit—Creek Crocodiles—to man the hostile creek area where India shares a border with Pakistan.

Role and Mandate the BSF:

- It guards Indo-Pak border,and Indo-Bangla border.
- The Cabinet Committee on Security (CCS) is considering a proposal to entrust the border-guarding duty along the Indo-Myanmar border to the Border Security Force (BSF). Presently, the 1,640 kilometres Indo-Myanmar border is being guarded by Assam Rifles. As of March 1st 2015, it was decided by the Ministry of Home Affairs to keep the authority of this border with Assam Rifles only.

1. **Peace time:**
   - Promote a sense of security among the people living in the border areas.
   - Prevent trans border crimes, unauthorized entry into or exit from the territory of India.
   - Prevent smuggling and any other illegal activity.
   - In the last few years the BSF has, in addition to their duties, been deployed for counter insurgency and internal security duties
2. **War Time:**
   - Holding ground in less threatened sectors so long as the main attack does not develop in a particular sector and it is felt that the local situation is within the capability of BSF to deal with.
   - The BSF units can continue to remain deployed in particular sector even in a war situation to release the Army for offensive tasks. In the even of a major attack developing, which is not within the capacity of the BSF to deal with, the Army can be expected either to reinforce the BSF with Artillery or other support, or relieve the BSF from its role in the particular sector.

- Protection of vital installations particular air-fields against enemy commandoes/para troopers or raids. The role can be entrusted to the BSF Units which are placed under the Army's operational Control.
- Limited Aggressive action against para military or irregular forces of the enemy within the overall plan of the Armed Forces .
- Performing special tasks connected with intelligence including raids. These are tasks which might be entrusted to BSF Units by the Army in a war situation according to local necessity.
- Acting as guides in an area of responsibility where routes are known.
- Maintenance of law and order in enemy territory administrated under the control of Army. Normally, ordinary civil police force would be utilised for this task but the BSF could be used to supplement the civil police or to act in lieu thereof in a situation where civil police is not readily available.
    - Guarding of prisoners of war cages
    - Assistance in control of refugees.
    - Anti – infiltration duties in specified area

Central Reserve Police Force (CRPF)

- Motto: Service and Loyalty
- Central Reserve Police Force Act, 1949
- The Central Reserve Police Force is the largest of India's Central Armed Police Forces.
- The Central Reserve Police Force came into existence as Crown Representative's Police on 27th July 1939. It became the Central Reserve Police Force on enactment of the CRPF Act on 28th December 1949.
- The CRPF is headed by a Director general who is an Indian Police Service officer.
- The CRPF has three battalions staffed entirely by women.

Role and Mandate of CRPF:

- It is a reserve force to assist state police in law and order
- Contain Insurgency
- Crowd Control
- VIP security
- Participate in UN peace keeping missions
- Environmental Protection

- Besides Law and Order and counter-insurgency duties, the role of CRPF in the General Elections, held repeatedly during the past few years, has been very significant and vital.
- It is also operating abroad as part of United Nations peacekeeping missions. It is performing a variety of duties ranging from VIP security to election duties, from guarding of vital installations to the counter-naxal operations.
- In recent years, the Government of India has decided to use each security agency for its mandated purpose. As a result, the counter-insurgency operations in India have been mainly entrusted to the CRPF.

Parliament Duty Group

- Parliament Duty Group is an elite CRPF unit tasked to provide armed protection to Parliament House.

Rapid Action Force (RAF)

- Motto: "Serving Humanity with Sensitive Policing"
- The Rapid Action Force (RAF) is a specialised wing of the CRPF. It was established on 11 December 1991 with headquarters in New Delhi, to deal with riots, riot like situations, crowd control, rescue and relief operations, and related unrest.
- The RAF is divided into two ranges headed by a DIGP at New Delhi and Mumbai.
- It currently has 10 specialised trained and equipped battalions, located at New Delhi, Mumbai, Ahemadabad, Bhopal, Aligarh, Meerut, Hyderabad, Jamshedpur, Coimbatore and Allahabad.
- The CRPF female and male contingents under the arrangements of RAF are deployed in United Nations Mission in Liberia (UNMIL), Monrovia and Zwedru in UN Peacekeeping mission since 2007-08. CRPF Female Formed Police Unit was the first of its kind in the world, which was deployed under the aegis of UN Peace Keeping Mission.

COBRA

- Motto: "Victory or Death"
- COBRA (COmmando Battalion for Resolute Action) is a specialised unit of the CRPF created in 2008 to counter the Naxalite problem in India.

- This specialised CRPF unit is one of the few units of the Central Armed Police Forces in the country who are specifically trained in guerilla warfare. This elite fighting unit has been trained to track, hunt and eliminate small Naxalite groups.
- Cobras are trained in the Army's elite Counter Insurgency and Jungle Warfare School in Mizoram and CRPF's anti terrorist school in Silchar. They are adept in the art of camouflage and jungle warfare.
- There are currently 10 COBRA units

Central Industrial Security Force (C.I.S.F)

- Motto: Protection and Security
- Central Industrial Security Force Act, 1968
- Its headquarters is at New Delhi. The CISF is headed by an Indian Police Service officer with the rank of Director-General.
- The CISF came into existence in 1969 with a modest beginning, having three battalions, to provide integrated security cover to the Public Sector Undertakings (PSUs).
- With globalization and liberalization of the economy, CISF is no longer a PSU-centric organization. Instead, it has become a premier multi-skilled security agency of the country, mandated to provide security to major critical infrastructure installations of the country in diverse areas.
- CISF is currently providing security cover to nuclear installations, space establishments, airports, seaports, power plants, sensitive Government buildings and ever heritage monuments. Among the important responsibilities recently entrusted to the CISF are the Delhi Metro Rail Corporation, VIP Security, Disaster Management and establishment of a Formed Police Unit (FPU) of the UN at Haiti.
- After the Mumbai terrorist attack on November 2008, the mandate of the force has been broadened to provide direct security cover to private sector also by amending the CISF Act.
- In CISF there are some reserved battalions which works with the state police to protect law and orders. CISF plays a major role in Disaster Management.
- Unique thing which the CISF has is a Fire Wing which helps during fire accidents in Industries where CISF is on guard.

Sashastra Seema Bal

- Motto: Service, Security and Brotherhood
- Sashastra Seema Bal Act, 2007
- It was formerly known as the Special Service Bureau
- Special Service Bureau (SSB) was set up in early 1963 in the wake of the Indo-China conflict to inculcate feelings of national belonging in the border population and develop their capabilities for resistance through a continuous process of motivation, training, development, welfare programmes and activities in the then NEFA, North Assam, North Bengal, hills of Uttar Pradesh, Himachal Pradesh, and Ladakh. The scheme was later extended to Manipur, Tripura, Jammu, Meghalaya, Sikkim, Manipur, Mizoram and some border areas of Rajasthan and Gujarat, South Bengal, Nagaland and Nubra Valley, Rajouri and Poonch district of Jammu and Kashmir.
- Pursuant to the recommendations of the Group of Ministers on reforming the National Security System, SSB was declared as a border guarding force and lead intelligence agency (LIA) for Indo-Nepal border (January, 2001) and Indo-Bhutan border(March, 2004). SSB was renamed as "Sashastra Seema Bal" in accordance with its new role and come under the administrative control of the Ministry of Home Affairs in January 2001. This was done after Kargil War when " one border one force concept" was adopted.

Role and Mandate of SSB:

- As a border guarding force and lead intelligence agency (LIA) for Indo-Nepal border and Indo-Bhutan border.
- To promote sense of security among the people living in the border area.
- To prevent trans-border crimes and unauthorized entries into or exit from the territory of India.
- To prevent smuggling and other illegal activities.

Indo-Tibetan Border Police Force

- Motto: Valour – Determination – Devotion to Duty
- Indo-Tibetan Border Police was conceived on October 24, 1962, , in the wake of the Sino-Indian War of 1962. ITBP was initially raised under the CRPF Act, however in 1992, the parliament enacted the ITBPF Act
- ITBP is a mountain trained Force. Forces are called "Himveer".

Role and Mandate of ITBPF:

- Presently, battalions of ITBP are deployed on border guard duties from Karakoram Pass in Ladakh to Diphu La in Arunachal Pradesh, covering 3488 km of the India-China border.
- ITBP is a multi-dimensional force which primarily has 5 functions:

1. Vigil on the northern borders, detection and prevention of border violations, and promotion of the sense of security among the local populace.
2. Check illegal immigration and trans-border smuggling
3. Provide security to sensitive installations and threatened VIPs
4. Restore and preserve order in any area in the event of disturbance
5. to maintain the peace
6. New challenging role that has emerged for ITBP is disaster management. Being the first responder for natural Disaster in Hamalayas, ITBP was the first to establish 06 (Now 08) Regional Response Centres in HP, Uttaranchal and North East and carried out numerous rescue and relief operations in various disaster situations. ITBP has established a National Centre for Training in Search, Rescue & Disaster response at Bhanu, Haryana which is imparting training to personnel of ITBP and other Paramilitary / State Police Forces. there is also a training center for the Dogs.
7. Presently ITBP Commando's are providing security to Embassy of India Kabul,Consulate General of India, Jalalabad and Khandar in Afghanistan since November, 2002. Besides this 02 Coys of ITBP are providing security to BRO personnel for their Delaram – Zaranj road construction project in Afghanistan since July 2004.
8. ITBP has also excelled in UN peace keeping operation. The Force personnel have been deployed for peacekeeping operations in Angola, Namibia, Cambodia, Bosnia & Herzegovina, Mozambique and Kosovo.
9. ITBP is also providing security to the pilgrims during Annual Kailash Mansarovar Yatra from 1981.
10. ITBP is in the forefront of movement for the preservation of Himalayan environment & ecology. Being the only human presence on forward areas, it has taken on itself the task of maintaining the delicate balance of flora and fauna.
11. ITBP being deployed in mountains has developed the expertise in rescue & relief operations
12. ITBP conducts a large number of medical civic action programmes in remote border and terrorist affected areas to provide free and expert medical, health and hygiene care to the civilian population in remote villages.

National Security Guard (NSG)

- Motto: (Sarvatra Sarvottam Surakhsha) Omnipresent Omnipotent Defense
- HQ: New Delhi.
- The National Security Guard (NSG) is a force under the Ministry of Home Affairs (MHA). It was raised in 1984, following Operation Blue Star and the assassination of Indira Gandhi, "for combating terrorist activities with a view to protect States against internal disturbances"
- NSG is headed by an Officer from IPS.
- Thus the primary role of this Force is to combat terrorism in whatever form it may assume in areas where activity of terrorists assumes serious proportions, and the State Police and other Central Police Forces cannot cope up with the situation. The NSG is a Force specially equipped and trained to deal with specific situations and is therefore, to be used only in exceptional situations. The Force is not designed to undertake the functions of the State Police Forces or other Para Military Forces of the Union of India.
- The NSG personnel are often referred to in the media as Black Cat Commandos because of the black dress and black cat sign-age worn on their uniform.
- The NSG's is trained to conduct counter terrorist task to including counter hijacking tasks on land, sea, and air; Bomb disposal (search, detection and neutralization of IEDs); PBI (Post Blast Investigation) and Hostage Rescue missions.
- In 26 November 2008 Mumbai attacks —NSG carried out Operation Black Tornado and Operation Cyclone to flush out terrorists & rescue hostages after multiple attacks across Mumbai.
- Post the 26/11 Mumbai terror strike, four regional hubs of NSG were operationalised in Mumbai, Hyderabad, Chennai and Kolkata to reduce reaction time.
- The NSG was modeled on the pattern of the SAS of the UK and GSG-9 of Germany. It is a task-oriented Force and has two complementary elements in the form of the Special Action Group (SAG) comprising Army personnel and the Special Ranger Groups (SRG), comprising personnel drawn from the Central Para Military Forces / State Police Force.

1. The SAG is the main offensive or the strike wing of the NSG.
2. SRG renders logistical support to the SAGs during operations and are deployed for guarding high-risk domestic and international VIPs/VVIPs. However VIP/VVIP Security is not mandate of NSG.

Railway Protection Force (RPF):

- The Force is under the authority of Ministry of Railways (India).
- The RPF Act, 1957
- RPF is headed by Director General who is usually an Indian Police Service officer.

Mandate:

- To protect Railway property.
- To do all conducive means for the free movement of the railways.
- Protection and safeguarding the passengers.

Special Protection Group (SPG)

- Motto: Bravery, Dedication, Security
- Special Protection Group Act, 1988
- The SPG was constituted and trained specially to provide protection to Prime Minister Rajiv Gandhi, in view of the threats to him from several sources. But, the organization created for the proximate security of Prime Minister Gandhi, did not contemplate provision of protection to him when he ceased to be Prime Minister, and faced magnified threats. SPG cover for Rajiv Gandhi was withdrawn once he ceased to be Prime Minister. After the assassination of Rajiv Gandhi in May 1991, the SPG Act was amended in 1991 to provide security to former Prime Ministers and their immediate families for a period of 10 years from the date on which the former Prime Minister ceased to hold office. Security could be provided even beyond 10 years as per threat perception.
- Family members of a serving Prime Minister (PM) may decline security. Former PMs and their immediate family members may also, if they choose, decline SPG security.
- The director of the SPG since its inception has been an officer from the Indian Police service. Personnel of the Special Protection Group are drawn from Central Armed Police Forces & Railway Protection Force.

National Disaster Response Force (NDRF):

- The National Disaster Response Force (NDRF) is a police force constituted "for the purpose of specialist response to a threatening disaster situation or disaster" under The Disaster Management Act, 2005.
- The "apex Body for Disaster Management" in India, is the National Disaster Management Authority (NDMA). The Chairman of the NDMA is the Prime Minister. The 'nodal Ministry' in the central government for management of natural disasters, is the Ministry of Home Affairs (MHA).
- National Disaster Response Force (NDRF) is a force of 12 battalions, organized on paramilitary lines, and manned by persons on deputation from the para-military forces of India: 3 BSF, 3 CRPF, 2 CISF, 2 ITBP and 2 Sashastra Seema Bal. The total strength of each battalion is approximately 1,149. Each battalion is capable of providing 18 self-contained specialist search and rescue teams of 45 personnel each including engineers, technicians, electricians, dog squads and medical/paramedics.
- NDRF in addition to being able to respond to natural disasters, has Four battalions capable of responding to radiological, nuclear, biological and chemical disasters.
- These NDRF battalions are located at nine different locations in the country based on the vulnerability profile to cut down the response time for their deployment. During the preparedness period/in a threatening disaster situation, proactive deployment of these forces will be carried out by the NDMA in consultation with state authorities.

Role and Mandate of NDRF:

- Specialized response during disasters
- Proactive deployment during impending disaster situations
- Acquire and continually upgrade its own training and skill
- Liaison, Reconnaissance, Rehearsals and Mock Drills
- Impart basic and operational level training to State Response Forces (Police, Civil Defence and Home Guards)
- Community Capacity Building Programmes
- Public Awareness Campaign
- Exhibitions : Posters, Pamphlets, literatures

12.VARIOUS CENTRAL INTELLIGENCE AGENCIES AND THEIR MANDATE

National Investigative Agencies (NIA)

- National Investigation Agency (NIA) is a federal agency established by the Indian Government to combat terror in India. It acts as the Central Counter Terrorism Law Enforcement Agency.
- The agency is empowered to deal with terror related crimes across states without special permission from the states. The Agency came into existence with the enactment of the National Investigation Agency Act 2008 by the Parliament of India on 31 December 2008.
- NIA was created after the 2008 Mumbai terror attacks as need for a central agency to combat terrorism was realised.

Special NIA Court:

- Various Special Courts have been notified by the Central Government of India for trial of the cases registered at various police stations of NIA under the NIA Act 2008. Any question as to the jurisdiction of these courts is decided by the Central Government. These are presided over by a judge appointed by the Central Government on the recommendation of the Chief Justice of the High Court with jurisdiction in that region.
- Supreme Court of India has also been empowered to transfer the cases from one special court to any other special court within or outside the state if the same is in the interest of justice in light of the prevailing circumstances in any particular state.
- The NIA Special Courts are empowered with all powers of the court of sessions under Code of Criminal Procedure, 1973 for trial of any offense.
- An appeal from any judgement, sentence or order of a Special Court lies to the High Court.

Role and Mandate:

1. In-depth professional investigation of scheduled offences using the latest scientific methods of investigation

2. Ensuring effective and speedy trial.
3. Developing into a thoroughly professional, result oriented organization, upholding the constitution of India and Laws of the Land giving prime importance to the protection of Human Rights and dignity of the individual.
4. Developing a professional work force through regular training and exposure to the best practices and procedures.
5. Displaying scientific temper and progressive spirit while discharging the duties assigned.
6. Inducting modern methods and latest technology in every sphere of activities of the agency.
7. Maintaining professional and cordial relations with the governments of States and Union Territories and other law enforcement agencies in compliance of the legal provisions of the NIA Act.
8. Assist all States and other investigating agencies in investigation of terrorist cases.
9. Build a data base on all terrorist related information and share the data base available with the States and other agencies.
10. Study and analyse laws relating to terrorism in other countries and regularly evaluate the adequacy of existing laws in India and propose changes as and when necessary.

National Crime Record Bureau (NCRB)

- The National Crime Records Bureau is an Indian government agency responsible for collecting and analysing crime data as defined by the Indian Penal Code (IPC). NCRB is headquartered in New Delhi and is part of the Ministry of Home Affairs (MHA). It was established in 1986.

Role and Mandate:

- To prepare an enabling IT environment – policy framework, guidelines, architecture, best practices for Police Forces throughout the country
- To improve knowledge based pro-active policing with the use of IT for improving internal efficiency, effectiveness and public service delivery.
- To create and maintain secure sharable National Databases on crimes, criminals, property and organized criminal gangs for law enforcement agencies and promote their use for public service delivery
- To obtain, compile, analyze and publish the National Crime Statistics

- To obtain, process and disseminate finger print records of criminals including foreign criminals to establish their identity; promote automation of State Finger Print Bureaux and encourage research for the development of Finger Print Science
- To provide training in IT and Finger Print Science for capacity building in Police Forces
- To coordinate development of Modern State Crime Records Bureaux
- To interact with Foreign Police Forces to share IT practices and crime information.

Narcotics Control Bureau (NCB):

- The Narcotics Control Bureau (NCB) is the apex coordinating agency, chief law enforcement and intelligence agency of India responsible for fighting drug trafficking and the abuse of illegal substances.
- The Director General of NCB is an officer of the Indian Police Service or the Indian Revenue Service. Headquarters is located in Delhi
- The National Policy on Narcotic Drugs and Psychotropic Substances is based on the Directive Principles, contained in Article 47 of the Indian Constitution, which direct the State to endeavour to bring about prohibition of the consumption, except for medicinal purposes, of intoxicating drugs injurious to health. The government's policy on the subject which flows from this constitutional provision is also guided by the international conventions on the subject.
- India is a signatory to the single Convention on Narcotic Drugs 1961, as amended by the 1972 Protocol, the Conventions on Psychotropic Substances, 1971 and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.
- The Narcotic Drugs and Psychotropic Substances Act, 1985 which came into effect from the 14th November, 1985 made an express provision for constituting a Central Authority for the purpose of exercising the powers and functions of the Central Government under the Act.
- In presence of this provision, the Government of India constituted the NARCOTICS CONTROL BUREAU on the 17th of March, 1986. The Bureau, subject to the supervision and control of the Central Government, is to exercise the powers and functions of the Central Government for taking measures with respect to:
    - Co-ordination of actions by various offices, State Governments and other authorities under the N.D.P.S. Act, Customs Act,

Drugs and Cosmetics Act and any other law in connection with the enforcement provisions of the NDPS Act, 1985. (like: Prevention of Illicit Trafficking in Narcotic Drugs and Psychotropic Substances Act, 1988.)

- Implementation of the obligation in respect of counter measures against illicit traffic under the various international conventions and protocols.
- Assistance to concerned authorities in foreign countries and concerned international organisations to facilitate coordination and universal action for prevention and suppression of illicit traffic in these drugs and substances.
- Coordination of actions taken by the other concerned Ministries, Departments and Organizations in respect of matters relating to drug abuse.

Directorate of Revenue Intelligence (DRI):

- DRI is the major intelligence agency which enforces prohibition of smuggling of drugs, gold, diamonds, electronics, foreign currency, counterfeit Indian currency, etc.
- The Directorate of Revenue Intelligence functions under the Central Board of Excise and Customs in the Ministry of Finance, Department of Revenue.

Role and Mandate:

- Collection of intelligence about smuggling of contraband goods, narcotics, under-invoicing etc. through sources of India and abroad, including secret sources.
- Analysis and dissemination of such intelligence to the field formations for action and working on such intelligence, where necessary.
- Keeping watch over important seizures and investigation cases.
- Associating or taking over the investigations which warrant specialized handling by the Directorate.
- Guiding important investigation / prosecution cases.
- Keeping liaison with foreign countries, Indian Missions and Enforcement agencies abroad on anti-smuggling matters.
- To keep liaison with C.B.I. and through them with the INTERPOL.
- To refer cases registered under the Customs Act to the Income Tax Department for action under the Income Tax Act.

- To keep statistics of seizures and prices/rates etc. for watching trends of smuggling and supply required material to the ministry of Finance and other Ministries.
- To study and suggest remedies for loopholes in law and procedures to combat smuggling.

Central Bureau of Investigation (CBI):

- Motto: "Industry, Impartiality, Integrity".
- At an early stage of World War-II, the Government of India realised that vast increase in expenditure for war efforts had provided opportunities to unscrupulous and anti-social persons, both officials and non-officials, for indulging in bribery and corruption at the cost of public and the Government. It was felt that Police and other Law Enforcement Agencies under the State Governments were not in a position to cope with the situation. An executive order was, therefore, passed by the Government of India in 1941, setting up the Special Police Establishment (SPE). Subsequently, Delhi Special Police Establishment Act, 1946 was brought into existence.
- The CBI was renamed the Central Bureau of Investigation on 1st April, 1963.
- CBI derives power to investigate from the Delhi Special Police Establishment Act, 1946. Section 2 of the Act vests DSPE with jurisdiction to investigate offences in the Union Territories only. However, the jurisdiction can be extended by the Central Government to other areas including Railway areas and States under Section 5(1) of the Act, provided the State Government accords consent under the Act.
- The CBI is under the control of Department of Personnel and Training of the Ministry of Personnel, Public Grievances and Pensions.
- The amended Delhi Special Police Establishment Act empowers a committee to appoint the director of CBI. (Selection committee was constituted under The Lokpal and Lokayuktas Act, 2013) The committee consists the following people:
    - Prime Minister – chairperson
    - Leader of Opposition – member
    - Chief Justice of India or a Supreme Court Judge recommended by the Chief Justice – member

Mandate of CBI:

- Cases in which public servants under the control of the Central Government are involved
- Cases in which the interests of the Central Government or of any public sector project or undertaking, or any statutory corporation or body set up and financed by the Government of India are involved.
- Cases relating to breaches of Central Laws with the enforcement of which the Government of India is particularly concerned, e.g.
    - Breaches of Import and Export Control Orders
    - Serious breaches of Foreign Exchange Regulation Act,
    - Passport frauds
    - Cases under the Official Secrets Act pertaining to the affairs of the Central Government.
    - Cases of certain specified categories under the Defence of India Act or Rules with which the Central Government is particularly concerned.
- Serious cases of cheating or fraud relating to the Railways, or Posts & Telegraphs Department, particularly those involving professional criminals operating in several States.
    - Crime on the High Seas
    - Crime on the Airlines
- Important and serious cases in Union Territories particularly those by professional criminals.
- Serious cases of fraud, cheating and embezzlement relating to Public Joint Stock Companies.
- Other cases of a serious nature, when committed by organized gangs or professional criminals, or cases having ramifications in several States, important cases of kidnapping of children by professional inter-state gangs, etc. These cases are taken up only at the request of or with the concurrence of the State Governments/Union Territories Administrations concerned.
- Collection of intelligence about corruption in the public services and the projects and undertakings in the public sector.
- Prosecution of cases investigated by this Division.
- Presentation of cases before Enquiry Offices in which departmental proceedings are instituted on
- the recommendation of CBI

Bureau of Police Research and Investigation (BPR&D):

- The Bureau of Police Research and Development (BPR&D) was set up on 28th August 1970 in furtherance of the objective of the Government of India for the modernisation of police forces.

Mandate:

- To Raise the Standards of Professionalism in Law Enforcement Policing
- To Optimally Blend Humanity with Technology to Produce Sustainable Institutional Cost – Efficient Outcomes.
- To Foster a Scientific, but humane, spirit of public-centric improvement in the Law Enforcement Policing and Prison Correctional Services across the country.
- To Devise Ways and Set Minimum Standards for Improving Police-Public Interface.
- To identify problems and needs of Police and initiate research in this field.

Multi Agency Centre

- MAC is a multi-agency centre for Counter Terrorism whose mandate is to share terrorism related inputs on a day-to-day basis.
- It was formed after Kargil War.

Intelligence Bureau (IB):

- The Intelligence Bureau (IB) is India's internal intelligence agency. IB is used to garner intelligence from within India and also execute counter-intelligence and counter-terrorism tasks.

Research and Analysis Wing (RAW):

- The Research and Analysis Wing (R&AW or RAW) is the primary foreign intelligence agency of India. It was created after the Sino-Indian War 1962 and Indo-Pakistani War of 1965 which exposed gaps in intelligence gathering undertaken by the Intelligence Bureau (which until then handled both domestic and foreign intelligence). This convinced the Government of India that a specialised, independent agency was required for foreign intelligence gathering.

- The primary function of R&AW is gathering foreign intelligence and counter-terrorism. In addition, it is responsible for obtaining and analysing information about foreign governments, corporations and persons to advise Indian policy makers. It is also involved in the security of India's nuclear programme.

NATGRID:

- The National Intelligence Grid or NATGRID is the integrated intelligence grid connecting databases of core security agencies of the Government of India to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies. It was first proposed in the aftermath of the terrorist attacks on Mumbai in 2008. NATGRID is being implemented in four phases, the first two of which will be operationalised by 2014.
- NATGRID is an intelligence sharing network that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel. This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing, the Intelligence Bureau, Central Bureau of Investigation, Financial intelligence unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Bureau, Central Board of Excise and Customs and the Directorate General of Central Excise Intelligence.
- NATGRID faced opposition on charges of possible violations of privacy and leakage of confidential personal information. Its efficacy in preventing terror have also been questioned given that no state agency or police force has access to its database thus reducing chances of immediate, effective action. NATGRID claims to be protected by several structural and procedural safeguards and oversight mechanisms including that of external audits.

National Counter Terrorism Center (NCTC)

- The National Counter Terrorism Center (NCTC) is a proposed federal anti-terror agency to be created in India, modelled on the National Counterterrorism Center of the USA. The proposal arose after the 2008 Mumbai attacks aka 26/11 attacks where several intelligence and operational

failures revealed the need for a federal agency with real time intelligence inputs of actionable value specifically to counter terrorist acts against India.

- The proposal has however met with much criticism from the Chief Ministers of various states who see this as a means of weakening India's federalism.

Central Forensic Institutes:

Central Forensic Science Laboratory (CFSL):

- The Central Forensic Science Laboratory (CFSL) is a wing of the Indian Ministry of Home Affairs, which fulfills the forensic requirements in the country.
- There are four central forensic laboratories in India, at Hyderabad, Kolkata, Chandigarh and New Delhi.
- These laboratories (except) are under the control of the Directorate of Forensic Science Services (DFSS) of the Ministry of Home Affairs. The laboratory in New Delhi is under the control of the Central Bureau of Investigation (CBI)

Directorate of Forensic Science Services:

The mandate of DFSS:

- To formulate plans, policies, and legislations to promote and regulate quality, capacity, and capability building for forensic services in the country.
- To facilitate high quality, on time and credible forensic services to the Homeland Security and Justice Delivery System.
- To encourage Research & Development activities
- To establish linkages with the national and international scientific and forensic institutions and universities for cooperation
- To disseminate knowledge on forensic services to the stake-holders by supporting/organizing training, awareness programmes, workshops and national/international conferences.
- To advise Central and State Governments in forensic matters and extend forensic assistance to manage national disasters/calamities.
- To develop National Forensic Information Grid (NAT-FORENS-GRID)
- To promote the concept of Quality Assurance and Quality Control in forensic services.

Central Finger Print Bureau

- CFPB is placed under the administrative control of the newly formed National Crime Records Bureau.
- The main functions of the CFPB have been mainly to maintain a database of fingerprint of criminals, National & International, and to disseminate the information.

13.RADIOLOGICAL AND NUCLEAR TERRORISM

Nuclear terrorism refers to an act of terrorism in which a person or people belonging to a terrorist organization detonates a nuclear device. Some definitions of nuclear terrorism include the sabotage of a nuclear facility and/or the detonation of a radiological device, colloquially termed a dirty bomb, but consensus is lacking. In legal terms, nuclear terrorism is an offense committed if a person unlawfully and intentionally "uses in any way radioactive material … with the intent to cause death or serious bodily injury; or with the intent to cause substantial damage to property or to the environment; or with the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing an act", according to the 2005 United Nations International Convention for the Suppression of Acts of Nuclear Terrorism.

The possibility of terrorist organizations using nuclear weapons (including those of a small size, such as those contained within suitcases) is something which is known of within U.S. culture, and at times previously discussed within the political settings of the U.S. It is considered plausible that terrorists could acquire a nuclear weapon. However, despite thefts and trafficking of small amounts of fissile material, all low-

concern and less than Category III Special nuclear material (SNM), there is no credible evidence that any terrorist group has succeeded in obtaining Category I SNM, the necessary multi-kilogram critical mass amounts of weapons grade plutonium required to make a nuclear weapon

Nuclear terrorism could include:

- Acquiring or fabricating a nuclear weapon
- Fabricating a dirty bomb
- Attacking a nuclear reactor, e.g., by disrupting critical inputs (e.g. water supply)
- Attacking or taking over a nuclear-armed submarine, plane, or base

Nuclear terrorism, according to a 2011 report published by the Belfer Center for Science and International Affairs at Harvard University, can be executed and distinguished via four pathways

- The use of a nuclear weapon that has been stolen or purchased on the black market
- The use of a crude explosive device built by terrorists or by nuclear scientists who the terrorist organization has furtively recruited
- The use of an explosive device constructed by terrorists and their accomplices using their own fissile material
- The acquisition of fissile material from a nation-state.
- The creation of a device that may give information about the configuration of components needed for a nuclear weapon

Former U.S. President Barack Obama called nuclear terrorism "the single most important national security threat that we face". In his first speech to the U.N. Security Council, President Obama said that "Just one nuclear weapon exploded in a city -- be it New York or Moscow, Tokyo or Beijing, London or Paris -- could kill hundreds of thousands of people". It would "destabilize our security, our economies, and our very way of life"

Militant groups

Nuclear weapons materials on the black market are a global concern, and there is concern about the possible detonation of a small, crude nuclear weapon by a militant group in a major city, with significant loss of life and property.

It is feared that a terrorist group could detonate a dirty bomb, a type of radiological weapon. A dirty bomb is made of any radioactive source and a conventional explosive. There would be no nuclear blast and likely no fatalities, but the radioactive material is dispersed and can cause extensive fallout depending on the material used. A foot-long stick of radioactive cobalt could be taken from a food irradiation plant and combined with ten pounds of explosives to contaminate 1,000 square kilometers and make some areas uninhabitable for decades. There are other radiological weapons called radiological exposure devices where an explosive is not necessary. A radiological weapon may be very appealing to terrorist groups as it is highly successful in instilling fear and panic among a population (particularly because of the threat of radiation poisoning) and would contaminate the immediate area for some period of time, disrupting attempts to repair the damage and subsequently inflicting significant economic losses.

al-Qaeda

According to *Bunn & Wier*, Osama bin Laden requested a ruling (a *fatwa*), and was subsequently informed via a cleric of Saudi Arabia during 2003, of it being in accordance with Islamic law for him to use a nuclear device against civilians if it were the only course of action available to him in a situation of defending Muslims against the actions of the U.S. military

According to leaked diplomatic documents, al-Qaeda can produce radiological weapons, after sourcing nuclear material and recruiting rogue scientists to build "dirty bombs". Al-Qaeda, along with some North Caucasus terrorist groups that seek to establish an Islamic Caliphate in Russia, have consistently stated they seek nuclear weapons and have tried to acquire them. Al-Qaeda has sought nuclear weapons for almost two decades by attempting to purchase stolen nuclear material and weapons and has sought nuclear expertise on numerous occasions. Osama bin Laden stated that the acquisition of nuclear weapons or other weapons of mass destruction is a "religious duty." While pressure from a wide range of counter-terrorist activity has hampered Al-Qaeda's ability to manage such a complex project, there is no sign that it has jettisoned its goals of acquiring fissile material. Statements made as recently as 2008 indicate that Al-Qaeda's nuclear ambitions are still very strong.

ISIS

ISIS has demonstrated ambition to use weapons of mass destruction. Although the chances of them obtaining a nuclear bomb are small, the group have been trying/suspected of trying to obtain a nuclear dirty bomb. In July 2014, ISIS militants

captured nuclear materials from Mosul University. In a letter to UN Secretary-General Ban Ki-moon, Iraq's UN Ambassador Mohamed Ali Alhakim said that the materials had been kept at the university and "can be used in manufacturing weapons of mass destruction". However, Nuclear experts regarded the threat as insignificant. International Atomic Energy Agency spokeswoman Gill Tudor said that the seized materials were "low grade and would not present a significant safety, security or nuclear proliferation risk".

In October 2015 it was reported that Moldovan authorities working with the FBI have stopped four attempts from 2010 to 2015 by gangs with suspected connections to Russia's intelligence services that sought to sell radioactive material to ISIS and other Middle Eastern extremists. The last reported case came in February 2015 when a smuggler with a large amount of radioactive caesium specifically sought a buyer from ISIS. The Criminal organizations are thriving on black market nuclear materials in Moldova. Since relations between Russia and the West have deteriorated, it is difficult to know whether smugglers are succeeding in selling radioactive material originating from Russia to Islamist terrorists and elsewhere.

In March 2016, it was reported that a senior Belgian nuclear official was being monitored by ISIS suspects linked to the November 2015 Paris attacks leading Belgium authorities to suspect that ISIS was planning on abducting the official to obtain nuclear materials for a dirty bomb.

In April 2016, EU and NATO security chiefs warned that ISIS are plotting to carry out nuclear attacks on the UK and Europe.

North Caucasus terrorists

North Caucasus terrorists have attempted to seize a nuclear submarine armed with nuclear weapons. They have also engaged in reconnaissance activities on nuclear storage facilities and have repeatedly threatened to sabotage nuclear facilities. Similar to Al-Qaeda, these groups' activities have been hampered by counter-terrorism activity; nevertheless they remain committed to launching such a devastating attack within Russia.

Aum Shinrikyo

The Japanese terror cult Aum Shinrikyo, which used nerve gas to attack a Tokyo subway in 1995, has also tried to acquire nuclear weapons. However, according to nuclear terrorism researchers at Harvard University's Belfer Center for Science and International Affairs, there is no evidence that they continue to do so.

Incidents involving nuclear material

Information reported to the International Atomic Energy Agency (IAEA) shows "a persistent problem with the illicit trafficking in nuclear and other radioactive materials, thefts, losses and other unauthorized activities".The IAEA Illicit Nuclear Trafficking Database notes 1,266 incidents reported by 99 countries over the last 12 years, including 18 incidents involving HEU or plutonium trafficking:

- There have been 18 incidents of theft or loss of highly enriched uranium (HEU) and plutonium confirmed by the IAEA.
- British academic Shaun Gregory alleged in 2009 that terrorists had attacked Pakistani nuclear facilities three times; twice in 2007 and once in 2008. However, the then Director General ISPR Athar Abbas said the claims were "factually incorrect", adding that the sites were "military facilities, not nuclear installations".
- In November 2007, burglars with unknown intentions infiltrated the Pelindaba nuclear research facility near Pretoria, South Africa. The burglars escaped without acquiring any of the uranium held at the facility.
- In June 2007, the Federal Bureau of Investigation released to the press the name of Adnan Gulshair el Shukrijumah, allegedly the operations leader for developing tactical plans for detonating nuclear bombs in several American cities simultaneously.
- In November 2006, MI5 warned that al-Qaida were planning on using nuclear weapons against cities in the United Kingdom by obtaining the bombs via clandestine means.
- In February 2006, Oleg Khinsagov of Russia was arrested in Georgia, along with three Georgian accomplices, with 79.5 grams of 89 percent HEU.
- In November 2006, the Alexander Litvinenko poisoning with radioactive polonium "represents an ominous landmark: the beginning of an era of nuclear terrorism," according to Andrew J. Patterson.
- In June 2002, U.S. citizen José Padilla was arrested for allegedly planning a radiological attack on the city of Chicago; however, he was never charged with such conduct. He was instead convicted of charges that he conspired to "murder, kidnap and maim" people overseas.
- There have been incidents where individuals such as David Hahn (aka the radioactive boy scout) and others have been initially charged under the relevant legislation due to the extent of contamination but the charges later withdrawn either due to lack of evidence or other reasons. This can be problematic when it is later proven that the intent was benign such as scientific research without the appropriate licenses or affiliation with an institution.

Pakistan

In 2009, a paper published in West Point Military Academy's journal alleged that Pakistan's nuclear sites had been attacked by al-Qaeda and the Taliban at least three times. However, Pakistan's military rejected the allegations. Talat Masood, a political analyst, said that the nuclear link was "absolute nonsense". All three attacks were suicide and appeared to aim at causing maximum damage and not seizing weapons. In January 2010, it was revealed that the US army was training a specialised unit "to seal off and snatch back" Pakistani nuclear weapons in the event that militants would obtain a nuclear device or materials that could make one. Pakistan supposedly possesses about 80 nuclear warheads. US officials refused to speak on the record about the American safety plans.

A study by the Belfer Center for Science and International Affairs at Harvard University titled "Securing the Bomb 2010," found that Pakistan's stockpile "faces a greater threat from Islamic terror groups seeking nuclear weapons than any other nuclear stockpile on earth." In 2016, Defense Intelligence Agency Director Vincent R. Stewart said that Pakistan "continues to take steps to improve its nuclear security, and is aware of the threat presented by extremists to its program".

According to Rolf Mowatt-Larssen, a former investigator with the CIA and the US Department of Energy, there is "a greater possibility of a nuclear meltdown in Pakistan than anywhere else in the world. The region has more violent extremists than any other, the country is unstable, and its arsenal of nuclear weapons is expanding." In 2015, White House press secretary Josh Earnest said that the US has confidence that Pakistan is "well aware of the range of potential threats to its nuclear arsenal". He added that the US is "confident that Pakistan has a professional and dedicated security force that understands the importance and the high priority that the world places on nuclear security".

Nuclear weapons expert David Albright and author of "Peddling Peril" has also expressed concerns that Pakistan's stockpile may not be secure despite assurances by both Pakistan and U.S. government. He stated that Pakistan "has had many leaks from its program of classified information and sensitive nuclear equipment, and so you have to worry that it could be acquired in Pakistan". In 2015, Richard G. Olson, former US Ambassador to Pakistan, expressed confidence in the capabilities of the Pakistani security forces to control and secure its nuclear weapons. He added that Islamabad has "specifically taken into account the insider threat".

A 2016 study by the Congressional Research Service titled 'Pakistan's Nuclear Weapons', noted that Pakistan's "initiatives, such as strengthened export control laws, improved personnel security, and international nuclear security cooperation programs, have improved Pakistan's nuclear security".

United States

President Barack Obama has reviewed Homeland Security policy and concluded that "attacks using improvised nuclear devices ... pose a serious and increasing national security risk". In their presidential contest, President George W. Bush and Senator John Kerry both agreed that the most serious danger facing the United States is the possibility that terrorists could obtain a nuclear bomb. Most nuclear-weapon analysts agree that "building such a device would pose few technological challenges to reasonably competent terrorists". The main barrier is acquiring highly enriched uranium.

In 2004, Graham Allison, U.S. Assistant Secretary of Defense during the Clinton administration, wrote that "on the current path, a nuclear terrorist attack on America in the decade ahead is more likely than not". In 2004, Bruce Blair, president of the Center for Defense Information stated: "I wouldn't be at all surprised if nuclear weapons are used over the next 15 or 20 years, first and foremost by a terrorist group that gets its hands on a Russian nuclear weapon or a Pakistani nuclear weapon". In 2006, Robert Galluccii, Dean of the Georgetown University School of Foreign Service, estimated that, "it is more likely than not that al-Qaeda or one of its affiliates will detonate a nuclear weapon in a U.S. city within the next five to ten years." Despite a number of claims, there is no credible evidence that any terrorist group has yet succeeded in obtaining a nuclear bomb or the materials needed to make one.

Detonation of a nuclear weapon in a major U.S. city could kill more than 500,000 people and cause more than a trillion dollars in damage. Hundreds of thousands could die from fallout, the resulting fires and collapsing buildings. In this scenario, uncontrolled fires would burn for days and emergency services and hospitals would be completely overwhelmed. The likely socio-economic consequences in the United States outside the immediate vicinity of an attack, and possibly in other countries, would also likely be far-reaching. A Rand Corporation report speculates that there may be an exodus from other urban centers by populations fearful of another nuclear attack.

The Obama administration will focus on reducing the risk of high-consequence, non-traditional nuclear threats. Nuclear security is to be strengthened by enhancing

"nuclear detection architecture and ensuring that our own nuclear materials are secure," and by "establishing well-planned, well-rehearsed, plans for co-ordinated response." According to senior Pentagon officials, the United States will make "thwarting nuclear-armed terrorists a central aim of American strategic nuclear planning." Nuclear attribution is another strategy being pursued to counter terrorism. Led by the National Technical Nuclear Forensics Center, attribution would allow the government to determine the likely source of nuclear material used in the event of a nuclear attack. This would prevent terrorist groups, and any states willing to help them, from being able to pull off a covert attack without assurance of retaliation.

In July 2010 medical personnel from the U.S. Army practiced the techniques they would use to treat people injured by an atomic blast. The exercises were carried out at a training center in Indiana, and were set up to "simulate the aftermath of a small nuclear bomb blast, set off in a U.S. city by terrorists."

Stuxnet is a computer worm discovered in June 2010 that is believed to have been created by the United States and Israel to attack Iran's nuclear facilities.

Nuclear power plants

After 9/11, nuclear power plants were to be prepared for an attack by a large, well-armed terrorist group. But the Nuclear Regulatory Commission, in revising its security rules, decided not to require that plants be able to defend themselves against groups carrying sophisticated weapons. According to a study by the Government Accountability Office, the N.R.C. appeared to have based its revised rules "on what the industry considered reasonable and feasible to defend against rather than on an assessment of the terrorist threat itself". If terrorist groups could sufficiently damage safety systems to cause a core meltdown at a nuclear power plant, and/or sufficiently damage spent fuel pools, such an attack could lead to widespread radioactive contamination. The Federation of American Scientists have said that if nuclear power use is to expand significantly, nuclear facilities will have to be made extremely safe from attacks that could release massive quantities of radioactivity into the community. New reactor designs have features of passive safety, which may help. In the United States, the NRC carries out "Force on Force" (FOF) exercises at all Nuclear Power Plant (NPP) sites at least once every three years.

The peace group Plowshares have shown how nuclear weapons facilities can be penetrated, and the groups actions represent extraordinary breaches of security at nuclear weapons plants in the United States. The National Nuclear Security Administration has acknowledged the seriousness of the 2012 Plowshares action.

Non-proliferation policy experts have questioned "the use of private contractors to provide security at facilities that manufacture and store the government's most dangerous military material".

Hoaxes

In late 1974, President Gerald Ford was warned that the FBI received a communication from an extortionist wanting $200,000 ($1,000,000 today) after claiming that a nuclear weapon had been placed somewhere in Boston. A team of experts rushed in from the United States Atomic Energy Commission but their radiation detection gear arrived at a different airport. Federal officials then rented a fleet of vans to carry concealed radiation detectors around the city but forgot to bring the tools they needed to install the equipment. The incident was later found to be a hoax. However, the government's response made clear the need for an agency capable of effectively responding to such threats in the future. Later that year, President Ford created the Nuclear Emergency Search Team (NEST), which under the Atomic Energy Act is tasked with investigating the "illegal use of nuclear materials within the United States, including terrorist threats involving the use of special nuclear materials".

One of its first responses by the Nuclear Emergency Search/Support Team was in Spokane, Washington on November 23, 1976. An unknown group called the "Days of Omega" had mailed an extortion threat claiming it would explode radioactive containers of water all over the city unless paid $500,000 ($2,200,000 today). Presumably, the radioactive containers had been stolen from the Hanford Site, less than 150 miles to the southwest. Immediately, NEST flew in a support aircraft from Las Vegas and began searching for non-natural radiation, but found nothing. No one ever responded despite the elaborate instructions given, or made any attempt to claim the (fake) money which was kept under surveillance. Within days, the incident was deemed a hoax, though the case was never solved. To avoid panic, the public was not notified until a few years later.

Policy landscape

Recovery

The Cooperative Threat Reduction Program (CTR), which is also known as the Nunn–Lugar Cooperative Threat Reduction, is a 1992 law sponsored by Senators Sam Nunn and Richard Lugar. The CTR established a program that gave the U.S. Department of Defense a direct stake in securing loose fissile material inside the since-dissolved USSR. According to Graham Allison, director of Harvard

University's Belfer Center for Science and International Affairs, this law is a major reason why not a single nuclear weapon has been discovered outside the control of Russia's nuclear custodians. The Belfer Center is itself running the *Project on Managing the Atom,* Matthew Bunn is a co-principal investigator of the project, Martin B. Malin is its executive director.

In August 2002, the United States launched a program to track and secure enriched uranium from 24 Soviet-style reactors in 16 countries, in order to reduce the risk of the materials falling into the hands of terrorists or "rogue states". The first such operation was *Project Vinca*, "a multinational, public-private effort to remove nuclear material from a poorly-secured Yugoslav research institute." The project has been hailed as "a nonproliferation success story" with the "potential to inform broader 'global cleanout' efforts to address one of the weakest links in the nuclear nonproliferation chain: insufficiently secured civilian nuclear research facilities."

In 2004, the U.S. Global Threat Reduction Initiative (GTRI) was established in order to consolidate nuclear stockpiles of highly enriched uranium (HEU), plutonium, and assemble nuclear weapons at fewer locations. Additionally, the GTRI converted HEU fuels to low-enriched uranium (LEU) fuels, which has prevented their use in making a nuclear bomb within a short amount of time. HEU that has not been converted to LEU has been shipped back to secure sites, while amplified security measures have taken hold around vulnerable nuclear facilities.

Options

Robert Gallucci, President of the John D. and Catherine T. MacArthur Foundation, argues that traditional deterrence is not an effective approach toward terrorist groups bent on causing a nuclear catastrophe. Henry Kissinger, stating the wide availability of nuclear weapons makes deterrence "decreasingly effective and increasingly hazardous." Preventive strategies, which advocate the elimination of an enemy before it is able to mount an attack, are risky and controversial, therefore difficult to implement. Gallucci believes that "the United States should instead consider a policy of expanded deterrence, which focuses not on the would-be nuclear terrorists but on those states that may deliberately transfer or inadvertently lead nuclear weapons and materials to them. By threatening retaliation against those states, the United States may be able to deter that which it cannot physically prevent."

Graham Allison makes a similar case, arguing that the key to expanded deterrence is coming up with ways of tracing nuclear material to the country that forged the fissile material. "After a nuclear bomb detonates, nuclear forensic cops would collect

debris samples and send them to a laboratory for radiological analysis. By identifying unique attributes of the fissile material, including its impurities and contaminants, one could trace the path back to its origin." The process is analogous to identifying a criminal by fingerprints. "The goal would be twofold: first, to deter leaders of nuclear states from selling weapons to terrorists by holding them accountable for any use of their own weapons; second, to give every leader the incentive to tightly secure their nuclear weapons and materials."

Nuclear skeptics

John Mueller, a scholar of international relations at the Ohio State University, is a prominent nuclear skeptic. He makes three claims: (1) the nuclear intent and capability of terrorist groups such as Al Qaeda has been "fundamentally exaggerated;" (2) "the likelihood a terrorist group will come up with an atomic bomb seems to be vanishingly small;" and (3) policymakers are guilty of an "atomic obsession" that has led to "substantively counterproductive" policies premised on "worst case fantasies." In his book *Atomic Obsession*: *Nuclear Alarmism from Hiroshima to Al-Qaeda* he argues that: "anxieties about terrorists obtaining nuclear weapons are essentially baseless: a host of practical and organizational difficulties make their likelihood of success almost vanishingly small".

Intelligence officials have pushed back, testifying before Congress that the inability to recognize the shifting modus oparandi of terrorist groups was part of the reason why members of Aum Shinrikyo, for example, were "not on anybody's radar screen." Matthew Bunn, associate professor at Harvard University's John F. Kennedy School of Government, argues that "Theft of HEU and plutonium is not a hypothetical worry, it is an ongoing reality." Almost all of the stolen HEU and plutonium that has been seized over the years had never been missed before it was seized. The IAEA Illicit Nuclear Trafficking Database notes 1,266 incidents reported by 99 countries over the last 12 years, including 18 incidents involving HEU or plutonium trafficking.

Keir Lieber and Daryl Press argue that despite the prominent U.S. focus on nuclear terrorism, "the fear of terrorist transfer [of nuclear weapons] seems greatly exaggerated... [and] the dangers of a state giving nuclear weapons to terrorists have been overstated." A decade of terrorism statistics show a strong correlation between attack fatalities and the attribution of the attack, and Lieber and Press assert that "neither a terror group nor a state sponsor would remain anonymous after a nuclear terror attack." About 75 percent of attacks with 100 or more fatalities were traced to the culprits; also, 97 percent of attacks on U.S. soil or that of a major ally (resulting

in 10 or more deaths) were attributed to the guilty party. Lieber and Press conclude that the lack of anonymity would deter a state from providing terrorist groups with nuclear weapons.

The use of HEU and plutonium in satellites has raised the concern that a sufficiently motivated rogue state could retrieve materials from a satellite crash (notably on land as occurred with Kosmos-954, Mars-96 and Fobos-Grunt) and then use these to supplement the yield of an already working nuclear device. This has been discussed recently in the UN and the Nuclear Emergency Search Team regularly consults with Roscosmos and NASA about satellite re-entries that may have contained such materials. As yet no parts were verifiably recovered from Mars 96 but recent Wikileaks releases suggest that one of the "cells" may have been recovered by mountain climbers in Chile.

Security summits

On April 12–13, 2010, President of the United States Barack Obama initiated and hosted the first-ever nuclear security summit in Washington D.C., commonly known as the Washington Nuclear Security Summit. The goal was to strengthen international cooperation to prevent nuclear terrorism. President Obama, along with nearly fifty world leaders, discussed the threat of nuclear terrorism, what steps needed to be taken to mitigate illicit nuclear trafficking, and how to secure nuclear material. The Summit was successful in that it produced a consensus delineating nuclear terrorism as a serious threat to all nations. Finally, the Summit produced over four-dozen specific actions embodied in commitments by individual countries and the Joint Work Plan. However, world leaders at the Summit failed to agree on baseline protections for weapons-usable material, and no agreement was reached on ending the use of highly enriched uranium (HEU) in civil nuclear functions. Many of the shortcomings of the Washington Nuclear Security Summit were addressed at the Seoul Nuclear Security Summit in March 2012.

According to Graham Allison, director of Harvard University's Belfer Center for Science and International Affairs, the objectives of the Nuclear Security Summit in Seoul are to continue to, "assess the progress made since the Washington Summit and propose additional cooperation measures to (1) Combat the threat of nuclear terrorism, (2) protect nuclear materials and related facilities, and (3) prevent illicit trafficking in nuclear materials."

14.BASICS OF CYBER SECURITY

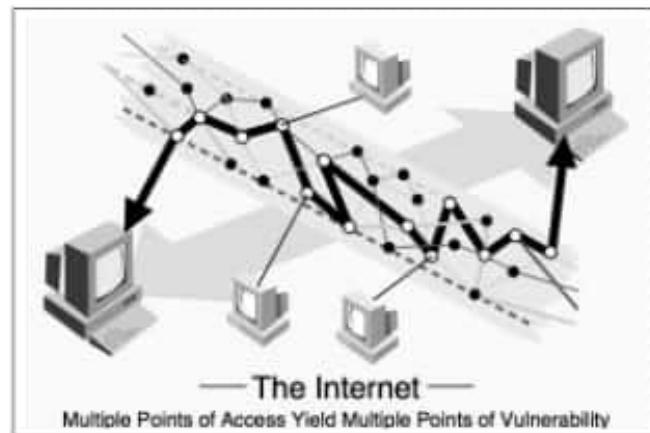
1. Introduction

Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. An increasing proportion of the world's population is migrating to **cyberspace** to communicate, enjoy, learn, and conduct commerce. It has also created new vulnerabilities and opportunities for disruption.

The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

Definition:

Cyber Security is "the security of information and its communicating channels as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole."

Cyberspace: It is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology devices and networks.

The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses.

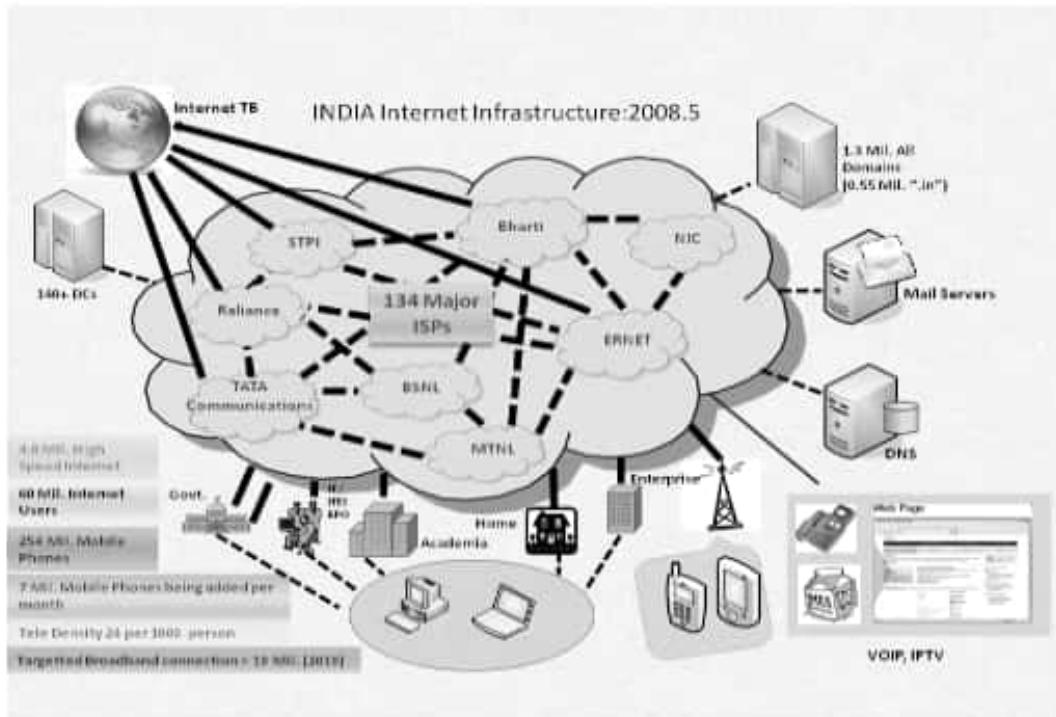
It has proved a challenge for governments all around the world. The task is made difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialized has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as a N/W created by academics for the use of the military, it has now become a global communications platform for socio-economic issues as well as for commercial and social purposes.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which,

- The number of Internet users has doubled between 2005 and 2010 and surpasses **2 billion**.
- Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage for several services.

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other.

2. The Indian Cyberspace

- The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government.
- Between 1986 and 1988, **three**N/Ws were set up:
  - **INDONET**, connecting the IBM mainframe installations that made up India's computer infrastructure;
  - **NICNET** (the NIC Network), being a nationwide very small aperture terminal (VSAT) N/W for public sector organisations as well as to connect the central government with the state governments and district administrations;
  - The Education and Research Network (**ERNET**), to serve the academic and research communities.
- Policies such as the **New Internet Policy of 1998** paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003.

Indian presence in Internet/Avenues of vulnerability in Cyber space / Indian stakes at risk in Cyber space

As per World Bank report

- By **June2012**,Internet users in India were approx. **12.5%** of the total population (approx. 137 million).

According to the Internet and Mobile Association of India (IAMAI),

- The internet user base in India is projected to touch **243 million** by **June 2014**, with a year-on-year growth of 28%.

This exponential growth is again expected to continue in recent future with more and more people accessing the web through mobile phones and tablets, with the government making a determined push to increase broadband(>4mbps) penetration from its present level of **about 6%.**

- *Thetwo top email providers, Gmail and Yahoo, had **over 34 million users** registered from India.*
- *62% of Internet users in India use Gmail.*
- *India's average connection speed is **1.3 mbps** (Nov 2013), the lowest among Asian countries. Compare that to China's 8.3 mbps and South Korea's 14.2 mbps.*
- *Only 2.4% of India's Internet connections have speeds >4 Mbps and barely 0.3% have 10 mbps or higher.*

National e-Governance Plan (NGeP)

Even though the Indian government was a late convert to computerization, there has been an increasing thrust on e-governance, seen as a cost-effective way of taking public services to the masses across the country.

Critical sectors such as Defence, Energy, Finance, Space, Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on N/Ws to relay data, for communication purposes and for commercial transactions.

The National e-governance Program (NeGP) is one of the most ambitious in the world and seeks to provide more than 1200 governmental services online. Schemes like *'Rajiv Gandhi scheme for broadband to PRIs'* and *National Optic Fiber Network (NOFN) mission*are already dedicated to accelerate cyber connectivity in far reaching areas of country.

- Under The National Broadband Plan, the target for broadband is **160 million households** by 2016. Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments.
- Similar level of penetration have also been seen in the social networking arena, which is the most recent entrant to the cyber platform.India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites.

*The number of Internet users in India increased from 1.4 million in 1998 to **100 million in 2010**. Internet penetration during this period rose from 0.1% to **8.5%**.*

Contribution of e-commerce to Economy

In terms of contribution to the economy,

- The contribution of the IT-ITES (BPO) industry to GDP increased from 5.2% in FY06 to around **8.0% in FY13**.
- The ICT sector has grown at an annual compounded rate of 33% over the last decade.
- An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India's top e-commerce retailer, saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million).
- The size of India's e-commerce market in 2013 was around **$13 billion**, according to a joint report of KPMG and Internet and Mobile Association of India (IAMAI).
- As per the same report, the e-commerce business in India is expected to reach around $50-70 billion by 2020 on the back of a fast growing internet-connected population and improvement in related infrastructure like payment and delivery systems.
- Currently estimated at **$2.3 billion** (about Rs 13,800 crores), Online Retailing is expected to gallop to almost **$38 billion** (Rs 2.27 lakh crores) in the next five years.

As India progresses, its reliance on the Internet will increase at a rapid pace. Globalization and governance require a wired society. Along with this India's vulnerability to the threat of Information War (IW) will become greater. This danger must be foreseen and planned for.

3. Cyberthreats

As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility.

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets:

1. Cyber Espionage,
2. Cyber Crime
3. Cyber Terrorism
4. Cyber Warfare

Cyber Espionage:

Cyber espionage, is "the act or practice of obtaining secret information without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware."

Simply said, Cyber espionage is "The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization."

Instances of cyber espionage are becoming quite common, with regular reports of thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and N/Ws of both government and private enterprises. It may also be that theft of intellectual property from private enterprises is not an issue here because R&D expenditure in India is only 0.7% of GDP, with government expenditure accounting for 70% of that figure.Though more recently, Cyber spying involves analysis of public activity on social networking sites like Facebook and Twitter. While government websites and NWs in India have been breached, theprivate sector claims that it has not been similarly affected. Companies are also reluctant to disclose any attacks and exfiltration of data, both b ecause they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public. As far as infiltration of government N/Ws and computers is concerned, cyber espionage has all but made **the Official Secrets Act, 1923** redundant, with even the computers in the Prime Minister's Office being accessed, according to reports.

India : Victim of Chinese Cyber Espionage

1. Cyber attack by Chinese crackers at the computers in the Prime Minister's Office(PMO) was reported in 2009.
2. In August 2015, security firm FireEye revealed an intense activity of hackers based in China particularly interested in entities and organization linked to the Indian Government as well as in information on Tibetan activists. The cyber espionage group sent targeted spear-phishing e-mails to its intended victims, with Microsoft Word attachments containing information on regional diplomatic issues .It said that collecting intelligence on India remains a key strategic goal for China-based APT groups, and these attacks on India and its neighbouring countries reflect growing interest in its foreign affairs.

The multiplicity of malevolent actors, ranging from state-sponsored to 'Hactivists', makes attribution difficult; governments currently can only establish measures and protocols to ensure **Confidentiality**, **Integrity** and **Availability** (CIA) of data.

Lately, it has been suggested to go on the Offensive against cyber spies and cyber criminals who are often acting in tandem with each other. But Offence is not necessarily the best form of defence in thecase of cyber security as perpetrators has not much to lose as compared to their counterparts in government.

USA DoJ (Department of Justice) brings **first-ever cyber-espionage case** against Chinese officials in **May 2014.** Chinese officials have been charged with hacking into major U.S. companies to steal trade secrets in order to compete with US.

Cyber Crime/ Cyber Attacks:

Cyber-attack is "any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an intention to damage or destroy targeted computer network or system."

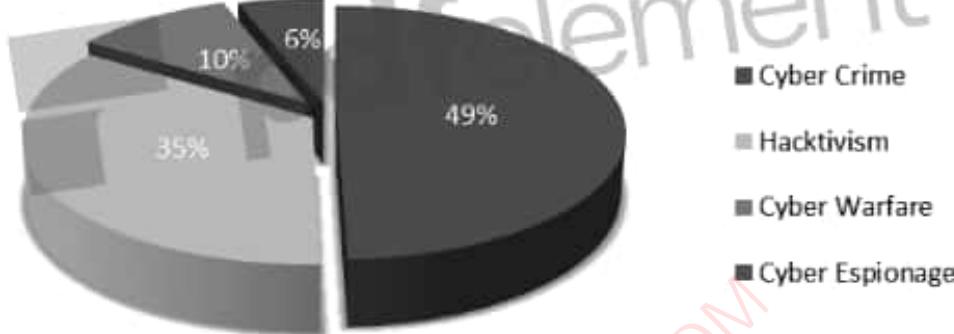
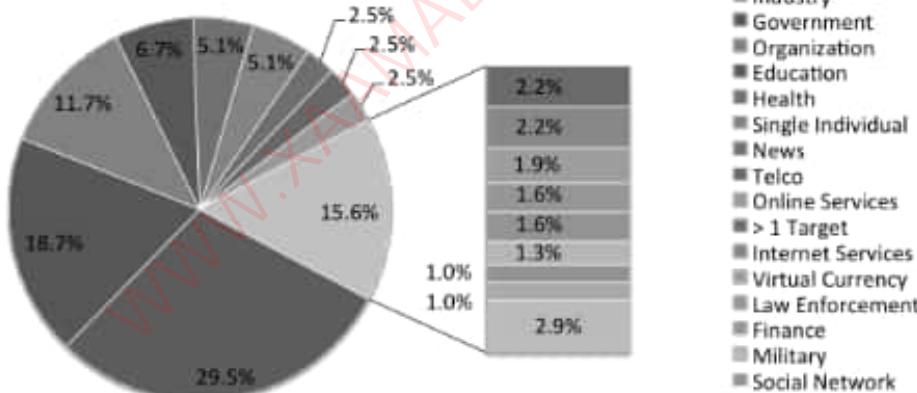
These attacks can be labeled either as Cyber-campaign, Cyber-warfare or Cyber-terrorism depending upon the context, scale and severity of attacks. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the critical infrastructure of entire nations.

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber-crime being in billions of dollars worldwide.

While other countries are reporting enormous losses to cyber-crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage.

- Though the report of the National Crime Records Bureau (NCRB) in 2010 reported an increase of 50% in cyber-crime over the previous year, the numbers were quite small in absolute terms.
- On 12 **July 2012**, a high profile cyber-attack breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organization (DRDO), and the Indo-Tibetan Border Police (ITBP).
- In **February 2013**, The Executive Director of the Nuclear Power Corporation of India (**NPCIL**) stated that his company alone was forced to block up to ten targeted attacks a day.

Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere .Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such as the establishment of the Data Security Council of India (DSCI) and the National Skills Registry. The Indian government has also aided these initiatives in a variety of ways, including deputing a senior police officer to NASSCOM to work on cyber security issues, keeping the needs of the outsourcing industry in mind.

Cyber attacks on Indian Government Websites

- As reported by Indian Computer Emergency Response Team (CERT-In) a total no. of 90, 119, 252 and 219 Government websites were defaced by various hacker groups in the year 2008, 2009, 2010 and January – October 2011 respectively
- 13000 incidents handled by CERT in in 2011

That said cyberspace is increasingly being used for various criminal activities and different types of cyber-crimes, causing huge financial losses to both businesses and individuals.

Organized crime mafia have been drawn to cyberspace, and this is being reflected in cyber-crimes gradually shifting from random attacks to direct (targeted) attacks. A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets . The vast amount of money lubricating this ecosystem is leading to increased sophistication of malicious codes such as worms and Trojans. The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars.

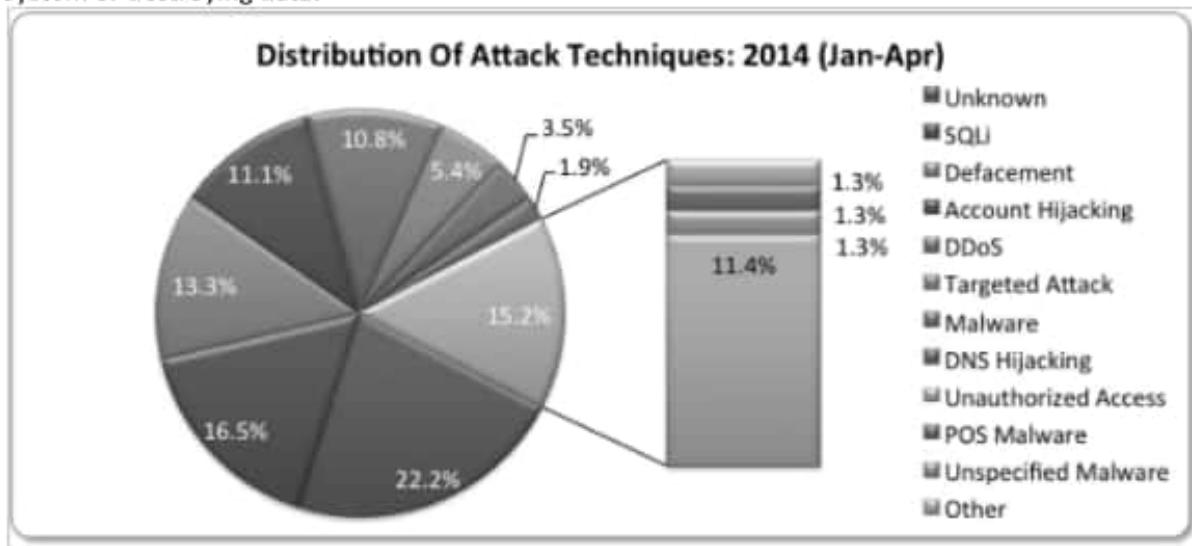
While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber-crime, as evinced by the increasing number of complaints on consumer complaint forums.

The low levels of computer security are also apparent in recurring statistics that show that India is the **third**-largest generator of spam worldwide, accounting for 35% of spam zombies and 11% of phishing hosts in the Asia-Pacific-Japan region.

A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average.

Methods of Attacks

Most popular weapon in cyber terrorism is the use of computer viruses and worms. Yet these attacks can be classified into three different categories

1. **Physical Attack** - using conventional methods like bombs, fire etc to harm the cyber infrastructure.
2. **Syntactic Attack** - The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.
3. **Semantic Attack** - This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors.

Tools of Cyber Attacks

Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware.

1. **Bluetooth hijacking –** (also called "*Bluejacking*") is an attack conducted on Bluetooth-enabled mobile devices, such as cellular telephones, smart phones, and PDAs.
2. **Botnet**- A botnet (a contraction of the term "RoBOTNETwork") is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. E.g. distribute malware, spam, and phishing scams etc.
    a. Network of compromised computers that are remotely controlled by malicious agents. They are used to send massive quantities of spam e-mail messages, co-ordinate distributed denial-of-service attacks (DDOS).
3. **Browser hijacking** - is the unintended modification of a web browser's settings by a malware. The term "hijacking" is used as the changes are performed without the user's permission. Some browser hijacking can be easily reversed, while other instances may be difficult to reverse. Various software packages exist to prevent such modification.
4. **Denials of service** (DoS) - an attack that prevents or impairs the authorized use of information system resources or services.These attacks are used to overwhelm the targeted websites. Attacks are aimed at denying authorized person's access to a computer or computer network.

5. **Distributed denial-of-service** (DDoS) - is a variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
6. **E-mail address harvesting** - obtaining an electronic mail address using an automated means from an Internet website or proprietary online service operated by another person.
7. **E-Mail Related Crime** - Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
    a. Cyber criminals are using **innovative social engineering techniques** through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. E.g. Nigerian email asking bank account to transfer lots of money. Tempting emails of user winning lottery or in some luck draw have been few famous tricks.
8. **Exploit tools** - publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain access into targeted systems.
9. **Hacking** - The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing tempest attack, password cracking and buffer outflow facilitates hacking, Identity theft.
10. **Logic bomb** - a computer program, which may perform some useful function, but which contains hidden code which, when activated, may destroy data, reformat a hard disk or randomly insert garbage into data files.
11. **Identity theft** - Obtaining and unlawfully possessing identity information of someone with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime.
12. **Keyboardlogging** - is a software that captures and "logs" every keystroke typed on a particular keyboard.
13. **Macrovirus –** is a program or code segment (can be called a Virus) written in the application's internal macro language.
14. **Malware -** (a concatenation of malicious software)a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.
15. **Pharming** – is a method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
16. **Phishing** - refers to a **social engineering attack**, where someone misrepresents their identity or authority in order to induce another person to provide personally identifiable information (PII) over the Internet.
17. **Root kit**–is a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
18. **Skimming** – is the act of obtaining data from an unknowing end user who is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus.
19. **Smart-card hijacking**
20. **Sniffer** - (also called a packet sniffer) is asoftware tool for auditing and identifying network traffic packets.
21. **Spamming** - unsolicited commercial e-mail (UCE) sent to numerous addressees or newsgroups.
22. **Spoofing** - the ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database.
23. **Spyware**- technologies deployed without appropriate user consent and/or implemented in ways that send away the information about user activity without his/her acknowledgement.
24. **SQLinjection** - is a way to cause database commands to be executed on a remote server. Such command execution can cause information leakage.
25. **Trojans** - Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12th Century BC.

26. **Virus –** A computer virus is the program code that attaches itself to application program and when application program run it runs along with it. It typically has a detrimental effect, such as corrupting the system or destroying data.

27. **War-dialing–** is a recursive dialing of phone numbers from a modem-enabled PC in an attempt to locate other unadvertised modems resulting in unauthorized access into a computing or Process Control System domain.
28. **War-driving** - is the recursive searching for wireless access points in an attempt to access a communication network resulting in unauthorized access into a computing or control system domain.
29. **Worms** - is a code that replicates itself and consumes the resources of a system to bring it down.
30. **Zero-day exploit** – is an attack against a software vulnerability that has not yet been addressed by the software maintainers. These attacks are difficult to defend against as they are often undisclosed by the vendor until a fix is available, leaving victims unaware of the exposure.

As per the **Verizon's 2014 Data Breach Investigations Report**, 92% of cyber-attacks in the past 10 years can be linked to just nine basic attack patterns. Top threat patterns identified by the report

1. Malware aimed at gaining control of systems
2. Insider/privilege misuse
3. Physical theft or loss
4. Web app attacks
5. Denial of service attacks
6. Cyber espionage
7. Point-of-sale intrusions
8. Payment card skimmers
9. Miscellaneous errors such as sending an email to the wrong person.

The scope and nature of threats and vulnerabilities is multiplying with every passing day.

Objectives of a cyber-attack

1. Loss of data integrity, such that information could be modified improperly.
2. Loss of data availability, where mission critical information systems are rendered unavailable to authorized users;
3. Loss of data confidentiality, where critical information is disclosed to unauthorized users; and,
4. Physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Benefits of Cyber-attacks

1. They are easy to use with high degrees of anonymity and with plausible deniability, making them well suited for covert operations and for instigating conflict between other parties;
2. They are more uncertain in the outcomes they produce, making it difficult to make estimates of deliberate and collateral damage; and
3. They involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of a second to years and at spatial scales anywhere from "concentrated in a facility next door" to globally dispersed.

Cyber terrorism:

Acts of Terrorism related to cyber space and /or executed using Cyber technologies is popularly known as 'cyber terrorism'.

Definitions of cyber terrorism

"Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear, Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact."

This is one of the most comprehensive definitions of cyber terrorism. But even this has a limitation. It states that for an attack to qualify as a cyber-terrorism it should lead to violence. This is more conventional. Terrorist may direct an attack only to disrupt key services, If they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous.

In the last couple of decades India has carved a niche for itself in IT. Most of the Indian banking industry and financial institutions have embraced IT to its full optimization. Reports suggest that cyber-attacks are understandably directed toward economic and financial institutions. Given the increasing dependency of the Indian economic and financial institutions on IT, a cyber-attack against them might lead to an irreparable collapse of our economic structures. And the most frightening thought is the ineffectiveness of reciprocal arrangements or the absence of alternatives.

Cyberspace has been used as a conduit by terrorists,

- For planning terrorist attacks,
- For recruitment of sympathizers,
- For Communication purposes
- For command and control
- Spreading propaganda in form of malicious content online to brain wash using their myopic ideological view
- For funding purposes
- As a new arena for attacks in pursuit of the terrorists' political and social objectives.

From that perspective, the challenges from non-state actors to national security are extremely grave. The shadowy world of the terrorist takes on even murkier dimensions in cyberspace where anonymity and lack of attribution are a given.

The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities especially in the aftermath of the terrorist attack in Mumbai in November 2008. Parliament passed

- 2008 amendments to the IT Act, with added emphasis on cyber terrorism and cyber-crime,
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act.

In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and National Security Requirements.

While **Cyber 'Hactivism'** cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of Cyberterrorism both in terms of methods and end goals.

Cyber Warfare: The Fifth domain of warfare

The evolution of technology impacts the nature of conflict and war. Cyber Warfare is a very recent yet evolving phenomenon.

In the absence of a formal definition of cyber warfare, we may define it as "*actions by a nation-state or its proxies to penetrate another nation's computers or networks for the purposes of espionage, causing damage or disruption*". These hostile actions against a computer system or N/W can take two forms: cyber exploitation and cyber-attacks.

Cyber exploitation is in a manner nondestructive and includes espionage. It is usually clandestine and is conducted with the smallest possible intervention that allows extraction of the information sought. It does not seek to disturb the normal functioning of a computer system or N/W. The best cyber exploitation is one that a user never notices. These are silent and ongoing, and as mentioned earlier, have shown an upward trend.

Cyber-attacks on the other hand are destructive in nature. These are deliberate acts of vandalism or sabotage – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy an adversary's computer systems or N/Ws or the information and programs resident in or transiting these systems or N/Ws.

Actors in both types of activities cover a wide range, as mentioned earlier. Of these, nation states and their proxies are of the greatest concern. For easier understanding, the domains of cyber warfare may broadly be classified as:

1. **Espionage** - Intelligence gathering and data theft. Examples of this were Titan Rain and Moonlight Maze. These activities could be by criminals, terrorists or nations as part of normal information gathering or security monitoring.
2. **Vandalism** - Defacing web pages or use DDOS to take them down. Such actions were evident in Estonia or Georgia.
3. **Sabotage** - This has the most serious implications and includes DDOS, destruction of data, and insertion of malware and logic bombs. It also encompasses actions in war such as those taken for preparation of the battlefield.

The Need to be Prepared

The growing threat of cyber warfare has not been well appreciated or sufficiently understood. Cyber warfare forms a part of Information War (IW), which extends to every form of media, and inter alia includes aspects of propaganda and perception management. Cyberspace, though technically restricted to the Internet, is now increasingly linked by convergence to every communication device. With greater connectivity, this divide is narrowing and every citizen or aspect of life is vulnerable. It is also an important constituent of **NCW** - amongst the recent aspects of involving in conflict is "No Contact War" (NCW) wherein there is no "physical" or "kinetic" action across borders.

> **A wakeup call !**
> Stuxnet, the cyber worm created by US' National Security Agency and Israeli military and posed a massive attack on the cyber infrastructure of Iran's nuclear enrichment centre at Natanz.
> Components of critical infrastructure such as
> - Programmable Logic Control (PLC) and
> - Supervisory Control and Data Acquisition (SCADA) systems were targeted by the Stuxnet malware that attacked supposedly secure Iranian nuclear facilities. Stuxnet exploited five distinct zero-day vulnerabilities in desktop systems, apart from vulnerabilities in PLC systems.
>
> Indian investigators had already found Stuxnet in Indian systems in early 2012.

The cyber realm, like the universe, is expanding and it is estimated that by 2015 there will be almost double the number of devices connected to the Internet as there are people. The scope for exploitation by inimical elements, ranging from mischievous hackers, to criminals, terrorists, non-state actors as also nation

states, is thus unlimited. The damage could be immense and many countries are pressing ahead and taking steps to build capabilities and capacities for defending themselves, as also taking offensive action in cyberspace.

- The United States was the first country to formally declare this as the fifth domain warfare after land, sea, air and space. It has also formally classified the use of cyberspace as a "force", a euphemism for offensive capability.
- The Chinese adopted the concept of "*informationalisation*" in the mid-1990s and have relentlessly built up structures and operations in this domain to stage a non-conventional threat to stronger inimical states.
    - In 2010 China overtly introduced its first department dedicated to defensive cyber warfare and information security in response to the creation of USCYBERCOM. The race is thus on.
- Consequent to the raising of the **US Cyber Command** (USCYBERCOM), South Korea followed with the creation of a Cyber Warfare Command in December 2009.
- The British Government Communications Headquarters (GCHQ) has begun preparing a cyber-force, as also France.

Recently NSA of India made a remark that "*India has a national cyber security policy not a national cyber security strategy*". This conveys all the concerns regarding lack of preparation for a Cyber warfare scenario.

Cyber Deterrence:

The **concept of cyber deterrence** is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution.

Cyber counter-intelligence

are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

Debate

- The issue whether cyber-attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated in global arena.

Multilateral discussions are veering around to debating whether there should be rules of behavior for state actors in cyberspace. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries.

There is, however, ongoing debate between those who believe that cyber warfare is over-hyped and those who believe that the world is heading towards a cyber-Armageddon. Both sides have valid arguments, but even as that debate continues, cyber warfare as a construct has become inevitable because the number of countries that are setting up cyber commands is steadily growing.

There is, therefore, a pressing need to think about norms for cyber warfare, whether the laws of armed conflict (LoAC) can be adapted to cyber warfare, and how principles like proportionality and neutrality play out in the cyber domain.

Indian initiative to combat Cyber-attacks/threats

India is a target. There have been numerous incidents of sensitive government and military computers being attacked by unknown entities and information being stolen. The frequency and intensity of such episodes is increasing. There is enough evidence to suggest that this is the action of nation states either directly or through proxies.

4. India's approach to Cyber Security:

1. Enabling Legal Framework
2. Cyber Security Policy
3. Compliance and Assurance
4. Cyber Security R&D Security
5. Incident – Early Warning and Response
   - National Cyber Alert System o
   - CERT-In and Sectoral CERTs o
   - Information Exchange with International CERTs
6. Security training
   - Skill & Competence development
   - Domain Specific training – Cyber Forensics, Network & System Security Administration
7. Collaboration
   - International
   - National

1. **Enabling legal framework** :
   The Information Technology **(IT) Act 2000**, later amendment in **2008**to define **Data Protection &Cyber crimes**.Information Technology (Amendment) Act, 2008 has been enacted and rules of important sections have been notified. The provisions of the Information Technology Act deal with evidentiary value of electronic transactions, digital signatures, cyber-crimes, cyber security and data protection.

Criminal Offences	Subsection
Sending offensive messages, including attachments, through communications service	66A
Dishonestly receiving stolen computer resource or communication device	66B
Identity theft	66C
Cheating by personating	66D
Violation of privacy	66E
Cyber terrorism: defined as causing denial of service, illegal access, introducing a virus in any of the **critical information infrastructure** of the country defined u/s 70 with the intent to threaten the unity, integrity, security or sovereignty of India or strike terror in the people or any section of the people; or gaining illegal access to data or database that is restricted for reasons of the security of state or friendly relations with foreign states.	66F
Publishing or transmitting of material containing sexually explicit act in electronic form	67A
Publishing or transmitting of material depicting children in sexually explicit act	67B
Preservation and retention of information by intermediaries as may be specified for such duration and in such manner and format as the central government may prescribe.	67C

Cyber Terrorism

- Sec 66 F: Punishment for Cyber Terrorism– (1)
  Whoever,–
  (A) with intent to threaten the unity, integrity, security or sovereignty of India or strike error in the people or any section of the people by–
  (i) deny or cause the denial of access to any person authorize to access computer resources; or
  (ii) attempting to penetrate or access a computer resource without authorization or exceeding authorised access; or
  (iii) introducing or causing to introduce any computer contaminant; or and by any means of such conduct causes o is likely to cause death or injuries to person or damage to or destruction of property or disrupts or knowing that it is likel to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70

5. National Cyber security Policy 2013

India released its first cyber security policy called National Cyber Security Policy in 2013.

The National Cyber Policy 2013 document outlines a road-map to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

Vision: To build a secure and resilient cyber space for citizen, businesses and Government.

Mission: To protect information and information infrastructure in cyberspace, build capacities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structure, people, process, technology and cooperation.

Objectives:

- To create secure cyber-ecosystem and enable adequate trust and confidence in electronic transactions and also guiding stakeholders actions for protection of cyber space.
- To create an assurance framework for design of security policies and enable actions for compliance of global standards.
- To strengthen regulatory framework for ensuring secure cyber ecosystem.
- To develop suitable indigenous technologies in ICT sector.
- To increase the visibility of integrity of ICT product by establishing infrastructure for testing and validation of security of such product.
- To create a workforce of 500,000 professionals skilled in cyber security in next five years.
- To provide fiscal benefits for corporate for adoption of cyber security.
- To safeguard the privacy of citizen's data.
- To enable effective prevention,detection and investigation of cyber crimes
- To create the culture of cyber security.
- To enhance global cooperation in cyber security

- To enhance protection and resilience of National Critical Information Infrastructure.
- To enhance national and sectoral 24*7 mechanisms for monitoring cyber threats.

Strategy:

1. **Creating a secure cyber ecosystem** :
    i. Designate nodal agency for coordination in cyber security related issues
    ii. Designate Chief Information Security Officer (CSIO) in all organization.
    iii. Encourage all organization to come out with cyber security policy in line with national policy
    iv. Ensure all organization allocate some part of their budget for cyber security
    v. Fiscal schemes for cyber security
    vi. Encourage trustworthy and indigenous ICT products.
2. **Creating assurance framework**:
    i. To promote adoption of best practices
3. **Encouraging open standards**
4. **Strengthening regulatory framework**
5. **Creating mechanisms for security threats early warning , vulnerability management and response to security needs**:
    i. Implement cyber crisis management plan.
6. **Securing e-governance services**
7. **Protecting and resilience of Critical Information Infrastructure**
8. **Promoting research and development in cyber security**
9. **Reducing supply chain risk**
    i. Create testing infrastructure and facilities for ICT products.
10. **Human resource development**
11. **Creating Cyber awareness**:
12. **Developing effective public private partnership**
13. **Information sharing and cooperation**
    i. Bilateral and multi lateral relationship in information sharing.
    ii. Enhance national and global cooperation
    iii. Mechanism for dialogue in the field of cyber security
14. **Prioritized approach for implementation**

The National Cyber Coordination Centre (NCCC)

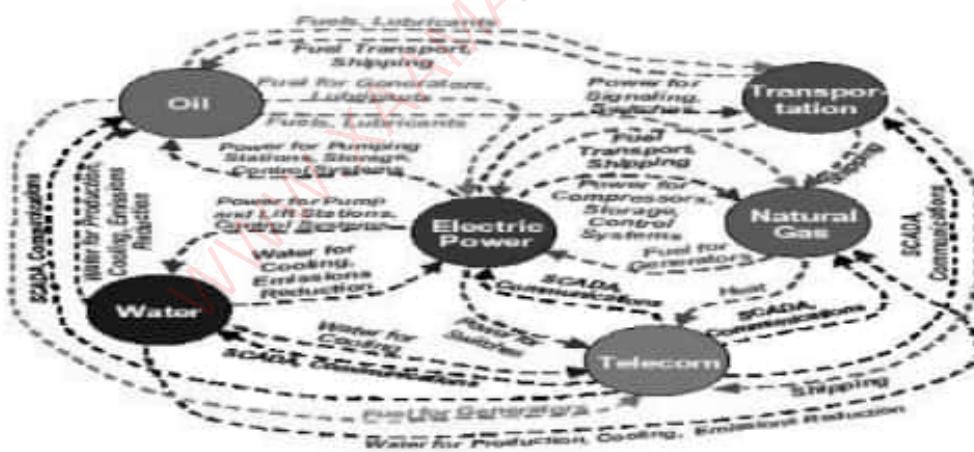
- Received an in-principle approval from the cabinet committee of security in May 2013 yet to become a reality.
- Will collect, integrate and scan [Internet] traffic data from different gateway routers of major ISPs at a centralized location for analysis, international gateway traffic and domestic traffic will be aggregated separately.
- The NCCC will facilitate real-time assessment of cyber security threats in the country and generate actionable reports/alerts for proactive actions by the concerned (law enforcement) agencies.
- Though the government won't say that they would be able to look into your Facebook or Twitter accounts as and when required, the fact remains that the setting up of the federal Internet scanning agency will give law enforcement agencies direct access to all Internet accounts, be it your e-mails, blogs or social networking data.
- Till now CERT-In was involved partially in this type of work although without intruding into any personal accounts.
- DG CERT-In is called **National cyber coordinator**. Now, the government is undecided on whom to appoint national cyber coordinator - the head of the NCCC.
- So far, CERT-IN has been the lead agency in signing agreements for better coordination with the international community.

The CERT-In (Cyber Emergency Response Team - India)

- Established in 2004, CERT-In function under DIT
- CERT-In is India's response to cyber threats and has following charter, mission and constituency.
- **Charter**: "*The purpose of the CERT-In is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur*"
- **Mission** "*To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.*"
- **Constituency**: The CERT-In's constituency is the Indian Cyber-community.
- is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security

Since **Nov 2012**, DG of CERT-In is called the **National Cyber Security Coordinator** (NCSC)

The NTRO (National Technical Research Organisation)

- Set up in 2004.
- Is a technical intelligence agency under the National Security Adviser in the Prime Minister's Office, India.
- It also includes National Institute of Cryptology Research and Development (NICRD)

Critical Information Infrastructure:

Background

Critical infrastructures are increasingly dependent on the information infrastructure for information management, communication and control functions. Certain information infrastructure or infrastructure sectors are of special importance.

According to Section 70(1) of the Information Technology Act 2000, Critical Information Infrastructure (CII) is defined as a "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

Complexity and Inter-dependence of CII

Critical Information Infrastructure (CII) is that ICT infrastructure upon which core functionality of Critical Infrastructure is dependent.

Among these Critical Information Infrastructures (CIIs) which are intricately interrelated and interdependent are

- Defense
- Space
- Banking and finance
- Power
- Transport
- Communications
- water supply
- Public Health
- Law enforcement agency
- Sensitive Government organizations
- Critical manufacturing
- E-Governance

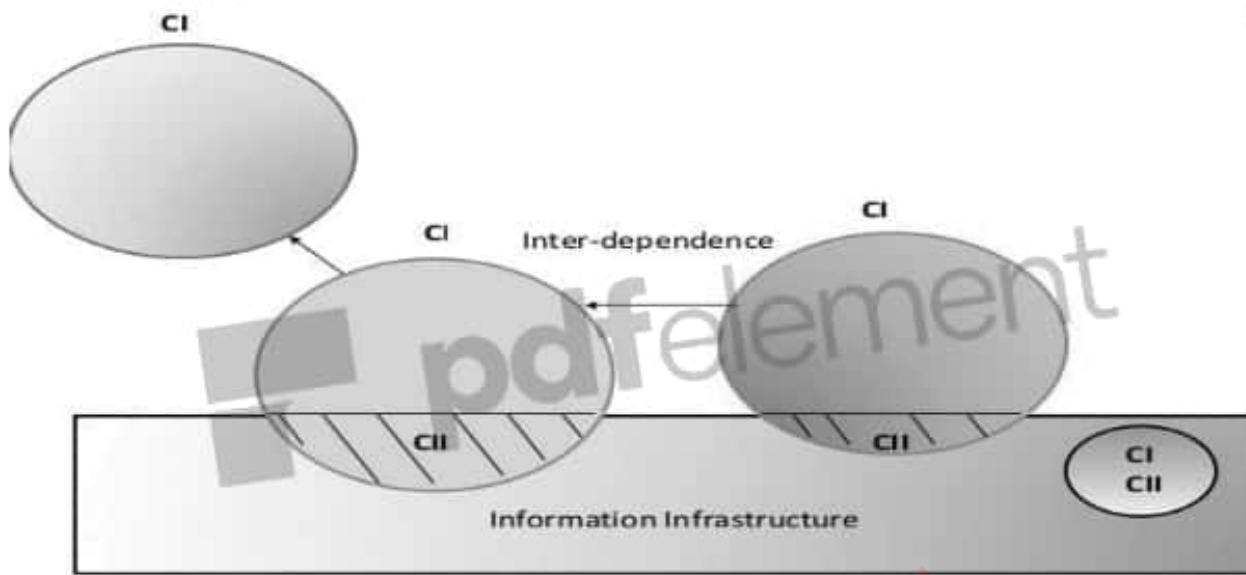



Figure: Varying Dependence of CI on Information Infrastructure

Sl No.	SECTOR as identified in crisis management plan 2010	Sub- sector	Dept./Agency Organization	Specific Area	Remarks
1.	Transportation	Civil aviation	AAI	ATC	Work under progress
2.	Transportation	Railways	IRCTC RAILTEL	Passenger reservation system, communication	Work under progress
3.	Transportation	Shipping	Port	Port management	
4.	Energy	Power	Powergrid corporation	POSOCO	Work under progress
5.	Energy	Nuclear	BAARC, NPCL		
6.	Energy	Oil & Gas	ONGC		
7.	Finance/Banking	Finance	NSE, BSE, Central Economic Intelligence Bureau (CEIB)	SIEN network (CEIB) NFS(National Financial Switches)	Work under progress
8.	Finance/Banking	Banking	SBI, RBI	INFINET, NEFT, SIEN	Work under progress
9.	ICT	Communication	MTNL, BSNL		Work under progress
10.	ICT	IT	NIC	NKN, SWAN	
11.	Law Enforcement, Security & intelligence	Law Enforcement & Security	ITBP, SSB, CRPF, Assam Rifles, BSF, CISF		
12.	Law Enforcement, Security & intelligence	Law Enforcement & Security	MHA	CCTNS	
13.	Law Enforcement, Security & intelligence	Intelligence Agencies	R&AW, IB, NTRO, CBI, NIA	NATGRID, FRRO Networks Cobweb	Work under progress
14.	Space	--	ISRO	Spacenet, Remote sensing, spacebased Programme	
15.	Defence	Army, Navy, Air Force, Coast guard, Strategic Forces Command			
16.	MEA	--	--	Passport Database/Visa	
		OTHERS			
17.	Sensitive Govt. Organisations	PMO, NSCS, Planning Commission, Cabinet Sectt., MHS, Registrar General Doordarshan & AIR		AADHAAR	Network from any of these areas which go through NIC

CHARACTERISTICS OF CII:

- Complex
- Distributed
- Interconnected
- Interdependent

- Threats to CII are classified as:
  - Internal Threat
    - It is defined as "One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm."
    - Insider betrayals cause losses due to IT sabotage, Fraud, and Theft of Confidential or proprietary information
    - This may be intentional or due to ignorance
  - External Threat
    - Arise from outside of the organization by individuals, hackers, organizations, terrorists , foreign Government agents, non state actors and pose risk like Crippling CII, Espionage, Cyber/Electronic warfare, Cyber Terrorism etc.

Effect of cyber attack on CII:

- Damage or Destruction of CII
- Disruption or Degradation of Services
- Loss of Sensitive / Strategic information
- Cascading Effect

6. National Critical Information Infrastructure Protection Centre (NCIIPC)

National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO) as the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures including associated Research and Development for the protection of CIIs in India.

NCIIPC - Key Responsibilities:

1. National Nodal Agency to protect NCII.
2. Deliver advice to reduce vulnerabilities.
3. Identify all CII elements for notification.
4. Provide strategic leadership and coherent Government response.
5. Coordinate, share, monitor, collect, analyse and forecast threats.
6. Develop plans, adopt standards, share best practices and refine procurement processes
7. Evolve protection strategies, policies, vulnerability assessment and auditing methodologies and plans for CII. 8. Undertake R&D to create, collaborate and develop technologies for growth of CII protection.
8. Develop training programs for CII protection.
9. Develop cooperation strategies.
10. Issue guidelines, advisories etc. in coordination with CERT-In and other organisations.
11. Exchange knowledge and experiences with CERT-In and other organisations. 13. NCIIPC may call for information and give directions to CII.

Any delay, distortion or disruption in the functioning of these CIIs can easily be lead to political, economic, social or national instability.

Taking telecommunications as a case in point, CII (**Critical Information Infrastructure**) in India comprises around 150 Internet and telecom service providers, offering Internet, mobile and wireless connectivity to a user base of nearly 800 million.

A major portion of data communication is facilitated by submarine cables .India has landing points for major submarine cable systems which are minimally protected. A preview of what could happen by way of these cables being disabled took place in 2008 when a series of outages and cable cuts in undersea cables running through the Suez Canal, in the Persian Gulf and Malaysia caused massive communications disruptions to India and West Asia.

Other sectors that could be subject to serious threats include the financial sector, which has largely transferred operations online. Stock exchanges in the United States and Hong Kong have reportedly been subject to cyber-attacks. The electricity grid is also vulnerable with the inevitable move towards a smart grid, given the economic and efficiency factors.

The protection of critical infrastructure is a complex task requiring forethought, planning, strong laws, technologies, PPP and resources. For all these reasons it needs to be given top priority by the government.

As in other countries, much of the infrastructure related to cyberspace is with the private sector. The government would necessarily have to work closely with the private sector, particularly in promoting cyber security practices and cyber hygiene

Compliance and Assurance:

1. Computer Security Guidelines have been circulated to all Departments and Ministries.
2. Cyber security drills are being conducted to assess preparedness of critical organisations.
3. 54 Auditors have been empanelled for audit of IT infrastructure from cyber security point of view.
4. Crisis Management Plan for countering cyber attacks and cyber terrorism has been released and is being updated annually. Enabling workshops are being conducted in different sectors and states/UTs.
5. Common Criteria (CC) product testing facility has been set up which caters up to level 4 CC certification. Controller of Certifying Authority (CCA) has licensed 7 Certifying Authorities (CA). More than 22 lakhs Digital Signature Certificates have been issued. Major Applications using
6. Digital Signatures include e-Procurement for Central and State Govt., e-Tendering, e-Filing of returns (MCA-21), Income Tax filing for corporate and individuals, Inter bank transactions (RTGS and SFMS), E-Filling of Patent Application and NSDL Applications.

Security Incident – Early Warning and Response:

1. A Computer Emergency Response Team –India (CERT-In) has been set up and is operational as the national agency for cyber incidents. It operates a 24x7 Incident Response Help Desk to help users in responding to cyber security incidents. It has been issuing regular alerts on cyber security threats and advises countermeasures to prevent attacks.
2. CERT-In has established linkages with international CERTs and security agencies to facilitate exchange of information on latest cyber security threats and international best practices. CERT-In, in collaboration with CII, NASSCOM and Microsoft, has created a portal "secureyourpc.in" to educate consumers on cyber security issues.

Cyber Security R&D:

A number of R&D projects have been supported at premier academic and R&D institutions in the identified Thrust Areas, viz.

a. Cryptography and cryptanalysis

b. Steganography
c. Network & systems security assurance
d. Network Monitoring
e. Cyber Forensics
f. Capacity Development in the area of cyber security. A host of Cyber Forensic tools have been developed in the country

Capacity Development/Training:

1. Training Centres have been set up at CBI, Ghaziabad and Kerala Police to facilitate advanced training in cyber crime investigation.
2. Computer forensic labs and training facilities are being set up in J&K state, North Eastern states. Forensic Centres have been set up with the help of NASSCOM at Mumbai, Bangalore, Bhopal and Kolkata. Virtual training environment based training modules have been prepared.
3. Training has been conducted for Orissa, Delhi, Andhra Pradesh and Karnataka Judicial Officers on Cyber Crime Investigation. 94 training 4 programmes have been conducted by CERT-In on specialized Cyber Security topics – in which 3392 people have been trained.

Collaboration:

1. As part of National level Cooperation, Cyber security awareness programmes were organised in cooperation with industry associations – CII, NASSCOM-DSCI. MoUs were signed with product and security vendors for vulnerability remediation. Several activities were undertaken under International Cooperation. International level Cyber security drills were held with Asia –Pacific CERTs.
2. Specific cyber security cooperation agreements were signed with US, Japan and South Korea. India participated in cyber security drills of US (Cyber Storm III).
3. CERT-In experts helped in establishment of CERT-Mauritius. India is participating in Internet traffic scanning in Asia-pacific region. India is a member of UN Committee of Group of Experts as well as in the Council of Security Cooperation in Asia-Pacific (CSCAP) for enhancing cooperation in the area of Cyber Security.

Current status of Cyber Security preparedness:

The initiatives taken by the Government so far have focused on the issues such as cyber security threat perceptions, threats to critical information infrastructure and national Security, protection of critical information infrastructure, adoption of relevant security technologies, enabling legal processes, mechanisms for security compliance and enforcement, Information Security awareness, training and research.

These actions have significantly contributed to the creation of a platform that is capable of supporting and sustaining the efforts to securing the cyber space. However, due to the dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time. Salient features of the results of actions and the level of cyber security preparedness include:

a) Information Technology (Amendment) Act 2008 has been enacted to cater to the needs of National Cyber Security by addressing host of issues such as technology related cyber crimes, critical information infrastructure protection, data security and privacy protection.
b) Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response. It has established operational linkages with overseas CERTs, and cyber security professional organisations to enhance its ability to respond to the cyber security incidents and take steps to prevent recurrence of the same.
c) PKI infrastructure, set up to support implementation of Information Technology Act and promote use of Digital Signatures, has enabled the growth and application of digital signature certificates in a number of areas. (d) National Crisis Management Plan for countering cyber attacks and cyber terrorism has been prepared and is being updated annually. Central Govt. Ministries/Departments and States and UTs as

well as organisations in critical sectors are making efforts to prepare and implement their own sectoral Crisis Management Plans.

d) To enable comprehensive cyber security policy compliance, the Govt. has mandated implementation of security policy within Govt. in accordance with the Information Security Management System (ISMS) Standard ISO 27001. In addition, Computer security guidelines have been issued for compliance within Govt. A Common Criteria based IT product security testing facility has been set up at Kolkata, which can test IT products up to EAL4.

e) A mechanism for audit and assessment of security posture of Govt. and critical sector organisations has been put in place. Security Auditors have been empanelled for conducting security audits including vulnerability assessment, penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations and those in other sectors of the Indian economy. Cyber security drills are being conducted regularly to assess the preparedness of organisations to resist and mitigate cyber attacks.

f) R&D activities have been supported through premier Academic and R&D Institutions in the country facilitating creation of R&D infrastructure, development skills and solution oriented development.

g) Nation-wide Information Security Education and Awareness Programme have been in progress to create necessary cyber security awareness through formal and informal programmes. Cyber security training facilities have been set up to provide training to law enforcement agencies and facilitating cyber crime investigation.

7. Need for an International Convention on Cyberspace

Cyber security is becoming an indispensable dimension of information security. The rapid growth of ICTs has contributed immensely to human welfare but has also created risks in cyberspace, which can destabilize international and national security. Additionally, the growth of social media (Twitter, Facebook, etc.) has created a new medium for strategic communication that by-passes national boundaries and national authorities.

The **global data transmission infrastructure** also depends critically on the N/W of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

Given the positive as well as negative potential of cyberspace, there has been talk of devising an **international convention on cyber security** which would ensure that states behave responsibly in cyberspace.

There already exist *several international conventions* (chemical weapons convention, biological toxins and weapons convention, NPT, etc.) and a body of international humanitarian law (Geneva and Hague conventions) from which inspiration can be drawn to build up a **Cyber Warfare Convention**.

A pressing question to be considered in the current unpredictable cyber scenario is the following.

- Should India actively engage itself in international efforts in framing a treaty or drawing up a framework of coherent cyber laws? Or, alternatively, should it wait till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes that may evolve as subsidiaries of a proposed cyberspace treaty?

Such a question has faced decision-makers right from the missile to nuclear technology control regime eras.

Opponents of a cyberspace-related treaty argue that even though the international efforts for harmonization of international legal frameworks for cyberspace do not refer to technology control regimes in their current manifestations, it would be just a matter of time before corollaries of such a treaty may emerge which would be based on technology control regimes; and signing such a treaty would result in undermining national sovereign interests. Similar arguments are brought up in respect of the European Convention on Cyber crime which, countries like Russia maintain, undermines their sovereignty.

The argument is that such treaties are biased in favour of the requirements of the major international players/powers and that India should stay aloof from such exercises till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes. But this type of isolationist approach is extensively

dependent on capability maturity model; and derives little or no benefit of the opportunities that can be capitalized by following an engagement model towards these treaties and conventions.

On the other hand, most of these cyber treaties are currently in their infancy and are undergoing development at various tier. If at this stage India proactively engages with the international community in drafting these cyber treaties and conventions, and capitalizes on this opportunity by mounding these cyber treaties and conventions to suit its sovereign interests, then the benefits achieved by the engagement approach would, without doubt, outweigh the potential outcomes of an isolationist approach.

Can there be a convention to govern cyber warfare, cyber weapons, use of force in cyber warfare, prevent cyber crime, etc.? As debate on these issues goes on, there is as yet no convention governing cyberspace.

A cyber convention would be unlike existing conventions in many ways. This is because in cyberspace attribution and identification is extremely difficult and identities can be easily masked. Cyber attacks also typically involve systems located in many countries. Often, cyber attacks are silent and go unnoticed for long periods.

UNGA has regularly passed resolutions on information security. Information security summits have been held in which cyber security has also been discussed. Several regional initiatives like the European Convention on Cyber crime have been in existence for decades. These efforts can be consolidated in the form of a cyberspace convention.

The key issues for consideration for a possible cyberspace convention would be:

1. National critical infrastructures should not be harmed.
2. Secure, stable and reliable functioning of the Internet should be ensured.
3. A common understanding of Internet security issues should be evolved.
4. National governments should have the sovereign right to make national policies on ICT consistent with international norms.
5. A global culture of cyber security based on trust and security should be encouraged.
6. The digital divide should be overcome.
7. International cooperation should be strengthened.
8. PPP should be encouraged.
9. CIA (Confidentiality – Integrity – Availability) of information systems should be ensured.
10. Balance between the need to maintain law and order and fundamental human rights should be maintained.

Such a convention would also define more precisely what constitutes threat in cyberspace and what would be the basic principles of information security.

- It would have many don'ts, as for instance the obligations on states not to take any overt or clandestine measures which would result in cyber warfare.
- It would also need to define what the use of force in cyberspace would mean and in what circumstances such force can be used, if at all.
- How would a state react if it is subjected to cyber attacks by a state, or a non-state actor, or by a combination of the two?
  - Given the nature of cyberspace, where attribution is difficult, these prohibitions will be hard to define and even harder to agree upon.

Arriving at a cyberspace convention would prove highly contentious. Yet, in India we need to debate openly the merits and demerits of the international law on cyberspace. Is such a convention possible at all? An Indian view needs to be evolved.

8. Digital Armed Force

Digital Army Programme:

Digital India:

The vision of Digital India programme is to transform India into a digitally empowered society and knowledge economy .It has nine pillars.

In keeping with the national vision of Digital India, the Indian Army has launched a program for Digital Army with nine pillars for digitisation. Three of the nine pillars of this umbrella program, namely Broadband highways, Universal access to telephones and Army Data Network stress upon Information Technology Infrastructure development. Another three namely e-Governance, Electronic delivery of services and Online information for all, focus on delivery of services to all units and formation headquarters. For any modern army, the Network Centric Operations are essential for meeting enhanced challenges of asymmetry, lethality, fluidity and non-linearity in the present day battlefield. The Indian Army is addressing this key area comprehensively.

Army and Digital India

The Army, since Independence, has lead the national effort in a number of ways and Digital India is a programme where it can become a lead contributor.

Some examples where the Army has already taken lead in building the Digital India vision are as under

- Network for Spectrum Optical Fibre project is a pan India network which will have the requisite band width for Broadband Highways.
- ARPAN 3.0, automation software for Army personnel, has been launched by the Defence Minister. It provides the Army personnel easy access to their service records, such as salary, leave, transfer and postings. This is digital empowerment of members of the Army.

The vision of Digital India can be the vision for all ranks of the Army too. Let us look into the role the Army can play in the 9 pillars of Digital India

- **Broadband Highways** – The Network for Spectrum Optical Fibre Network is already being implemented on ground and will provide the backbone infrastructure required for Broadband Highways. It should be feasible to cover this network right down to battalion level.
- **Universal Access to Mobile Connectivity** – The booming mobile phone industry is enabling access to Smart Phones to all citizens of the country. This is making it possible for all ranks of Armed Forces to have access to Smart Phones. Armed Forces would have a role to play to ensure that mobile tower infrastructure is given access in defence areas to enable Armed Forces personnel to access mobile communications.

- **Public Internet Access Program** – Internet today is becoming a necessity for all citizens. The mobile service providers are already providing this service on mobile phones. The issue of providing free wi-fi hotspots in military areas will have to be examined from the security point of view. It is possible to provide Internet access to all ranks with suitable security instructions and a monitoring mechanism without impinging on privacy.
- **eGovernance** – In respect of Army, this would imply providing administrative services in e-format. This is one area where Army needs to work a lot. Our services, for example in Cantonments, are still paper based with large lead times. Army needs to make an e-governance task force to steer this on a fast track basis. Another aspect which needs consideration is to provide all ranks access to their home station eGovernance portal from their place of posting. This will ease a large number of their problems.
- **e-Kranti** – With expectations on the rise ,eKranti is another area where the Army can make a difference for its personnel. Some areas of activity can be
    - **e-Education** – All training institutions can be interconnected and Digital based education can be provided. We can develop pilot projects on Massive Online Open Courses (MOOCs). Some work is already underway in this field.
    - **e-Healthcare** – Healthcare is an area which can have a revolutionary effect. Online medical records, Pan India exchange of patient information, online consultation etc are few of the many possibilities in improving health care access to all personnel.
    - **GIS** – Armed Forces can be part of the National GIS Mission Mode Project and use its facilities for GIS based decision making.
    - **Security** – Technology can be leveraged to improve security, something which is a necessity as far as Army is concerned. Cyber Security needs to be given the impetus required to safeguard us from Cyber Threats.
    - **Financial Inclusion** – We are aware that majority of our personnel are financially illiterate and have limited access to financial services. Financial inclusion will help personnel posted in field areas to easily transfer money and do a host of financial transactions without having to visit government offices/banking institutions.
- **Information for All** – The Army has already taken a number of measures to provide information to all ranks on both the Army Intranet and the internet. The Army can easily work towards providing more valuable information to all ranks.
- **Electronics Manufacturing** – Majority of the Indian Army weapon platforms are imported. Key components of these imports are electronics. The Army can contribute towards the aim of net zero import by 2020 by closely working with the industry to source electronics items from local manufacturers.
- **IT for Jobs**- While the aim of IT for jobs is make an IT ready workforce, Army also needs to train all personnel in the IT domain. It will help them being IT literate as well as make them industry ready when they leave the Army.
- **Early Harvest Programme** -The programme can be utilised by the Armed Forces as under
    - **Wi-Fi in all Universities** – For the Army, this can be implemented as Wi-Fi for all Training establishments. Wi-Fi access in Training establishments is feasible with fewer security issues.
    - **Secure email within Government** – The process of providing government emails has already commenced. Army can fast track this process to ensure that all authorised users are provided secure Government email, which in turn would become the primary mode of communication outside of the Army Intranet. It will enable official communications to move away from Gmail, Yahoo Mail etc
    - **Standardised Government email Design** – As is being done by the government, we will also have to design our email design templates as per our requirements .While such templates are already functional in the Army intranet, templates where mail has to be sent by internet needs to be worked out.

As brought out above, it is highly feasible to implement the Digital India program within the Army. To play a lead and a contributory role in implementation and success of the Digital India program, the Army needs to build an ecosystem which takes the programme forward. While it will not be feasible to raise a new organisation to steer it forward, it is possible to nominate an establishment as the nodal agency for monitoring and progressing

implementation of the program. Actual implementation responsibility can be given to different directorates/branches/commands as per tasks involved. It would also require the Army to co-opt other organisations like DRDO, other branches of government as required, sister services (Air Force and Navy) etc to efficiently implement this program. The canvas of Digital India in the Army is enormous. It only requires imagination and drive to make this an enormous facilitator for all ranks of the Army.

Security

In the overall gambit of implementing Digital India in the Army, the biggest concern would be security. Security is something which will remain paramount to the Army and it is here that some disconnect in its implementation may exist. In the civil arena, generally, implementation comes first and security follows based on security breaches, security alerts etc. whereas in the Army, security precedes implementation of programmes. That is the reason that world over, the networks, communication systems, etc of the Army are a generation behind the civil industry. On the positive side, there are a number of components of the Digital India program which can be easily implemented without any major security issue.

Digital India provides an opportunity for the Army to lead the effort in developing and integrating security in the Digital India infrastructure. Army, sister services, DRDO and other Research and Development agencies can get together to take this effort forward. This effort has to be in house as security cannot be outsourced.

Conclusion

Digital India is an umbrella program to provide efficient services to all citizens. Army can utilise this opportunity to make the program accessible to all ranks. Some organisations within the Army are already implementing few aspects of the Digital India. All the Army needs to do is to also create an umbrella organization to efficiently implement this program and not let it remain in individual silos.

NATIONAL ENCRYPTION POLICY Draft controversy :

Under Section 84A of Information Technology Act, 2000 Rules are to be framed to prescribe modes or methods for encryption. In this regard, a draft National Encryption Policy was formulated by an Expert Group setup by Government.
The aim was to enable information security environment and secure transactions in Cyber Space for individuals, businesses, Government including nationally critical information systems and networks.

Objective of the Policy:

To synchronize with the emerging global digital economy / network society and use of Encryption for ensuring the Security / confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safetyand National Security.

- To encourage wider usage of Digital Signature by allentities including Government for trusted communication, transactions and authentication.
- To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that are consistent with industry practice.

Need for encryption policy?

India needs a policy on encryption to provide guidance on the use of information/ data within the country in a regulated manner and ensure that our government agencies can access them for investigating serious issues related to terrorism, national security and critical infrastructure.

What is Encryption?

It is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted.

What is the purpose of encryption?

It is to ensure that only somebody who is qualified to access data (e.g. a text message or a file) will be able to read it, using the decryption key. Somebody who is not qualified to access the information can be excluded from doing that, because he does not have the required decryption key. Without it, it's impossible to read the encrypted information.

In that way, it's possible to protect random people from reading private information.

3 different encryption methods

There are **three** different basic encryption methods, each with their own advantages

- **Hashing**
  Hashing creates a unique, fixed-length signature for a message or data set. Each "hash" is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be reversed or deciphered. Hashing, then, though not technically an encryption method as such, is still useful for proving data hasn't been tampered with.
- **Symmetric methods**
  Symmetric encryption is also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (the ciphertext) and then the receiver uses the key to decrypt the data.
- **Asymmetric methods**
  Asymmetric encryption, or public-key cryptography, is different than the previous method because it uses two keys for encryption or decryption (it has the potential to be more secure as such). With this method, a public key is freely available to everyone and is used to encrypt messages, and a different, private key is used by the recipient to decrypt messages.

9. Draft National Encryption Policy

I. **Vision**

To enable information security environment and secure transactions in Cyber Space for individuals, businesses, Government including nationally critical information systems and networks.

II. **Mission**

To provide confidentiality of information in cyber space for individuals, protection of sensitive or proprietary information for individuals & businesses, ensuring continuing reliability and integrity of nationally critical information systems and networks.

III. **Objectives**

i) To synchronize with the emerging global digital economy / network society and use of Encryption for ensuring the Security / confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safety and National Security.

ii) To encourage wider usage of Digital Signature by all entities including Government for trusted communication, transactions and authentication.

iii) To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that are consistent with industry practice.

Salient features

- All citizens "*are required to store the plain text of the encrypted messages for 90 days*" and provide it to law enforcement agencies as and when required.
- All vendors of encryption products need to register their products with the designated agency of the Government
- All encryption technology used in India shall be cleared by the government
- Government shall maintain a list of all encryption technologies and only those technologies which are on the list can be used in this country. It means government knows every encryption technology used in India
- Common use Web-based applications and social media sites such as WhatsApp, Facebook and Twitter were exempted
- The encryption products being used in Internet-banking and payment gateways under direction of the RBI And those being used for e-commerce and password- based transactions, are also exempted.
- Research and Development programs will be initiated for the development of indigenous algorithms and manufacture of indigenous products for Encryption, hashing and other cryptographic functions.

Problem with draft:

1. Policy will affect almost all Internet users- a majority is not even aware that it is using encryption technologies.
2. The biggest concern of this new policy is around the fact that users and organizations would "*on demand*" need to store all communication in plain text for 90 days from the date of transaction and make it available to law enforcement agencies. Most of the users in India do not know the meaning of plain text and in such a case they can be held liable for not storing their encrypted data in plain text format. Thus, almost everyone using the Internet will find themselves in violation of these rules.
3. In case of communication with any foreign entity, the primary responsibility of providing readable plaintext along with the corresponding encrypted information shall rest on the business or citizen located in India.
4. Additionally, service providers located within and outside India, using encryption technology for providing any type of services in India, must enter into an agreement with the government. This is seen as impractical as there are many service providers around the world that use encryption. It would be highly unrealistic for all of these to enter into an agreement with the Indian government.
5. Keeping a copy of the data will require huge storage and that will come at a cost.
6. There is a fear that the policy will start a new "registration raj", now that all encryption technologies that can be used in India will need to be certified and listed by the agencies concerned.
7. For companies that store private data it would mean storing passwords in plain text, which means private and confidential data will remain unencrypted and hence vulnerable for 90 days.
8. The government proposed to prescribe the algorithms and key sizes for encryption. This implies government control over all data.

10. Smart Cities and Cyber Threats:

Cities are incorporating new technologies at an increasingly rapid pace, becoming ever smarter. Newer technologies — along with faster and easier connectivity — allow cities to optimize resources, save money and provide better services to their citizens. Cities around the world — whether considered smart or not — face significant cyber security threats. These problems could have a direct impact on government, residents and the companies and organizations doing business there. Cyber security in cities is extremely important, but we have

yet to fully realize the risk. Imagine what could happen if one or more technology-reliant services stopped working. What would commuting look like with no working traffic control systems, street lights or public transportation? How would citizens respond to an inadequate supply of electricity or water, dark streets and no cameras? What if waste collection was interrupted during the summer?

These scenarios might not be as unlikely as you think. There are many cyber security problems that could trigger them, such as:

- Lack of Cyber Security Testing Poor
- Encryption Issues
- Lack of Computer Emergency Response Teams
- Large and Complex Attack Surfaces
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Lack of Cyber Attack Emergency Plans
- Susceptibility to Denial of Service
- Technology Vendors Who Impede Security Research